บทที่ 2
เอกสารและทฤษฎีที่เกี่ยวข้อง

ในยุคที่เครือข่ายอินเทอร์เน็ตเป็นเสมือนปัจจัยพื้นฐานในการสื่อสารข้อมูลขององค์กร กับภายนอกองค์กร ซึ่งในเครือข่ายขนาดใหญ่นี้ มีการเชื่อมโยงระบบเครือข่ายทั่วโลกเข้าหากันจน เป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่สุดในโลกมีคนใช้บริการนับล้านคนเพื่อติดต่อสื่อสารกัน โอกาสของผู้ไม่ประสงค์ดีที่เข้ามารบกวนหรือทำลายระบบเครือข่ายภายในขององค์กรมีอยู่ ตลอดเวลา ซึ่งนับเป็นปัญหาที่มีผลกระทบกับการทำงานของหลายๆองค์กรในปัจจุบัน

2.1 ความสำคัญของการรักษาความปลอดภัยสำหรับระบบเครือข่ายคอมพิวเตอร์

แนวโน้มปัญหาเรื่องความปลอดภัยในระบบเครือข่ายขององค์กรที่ต่อเชื่อมกับ เครือข่ายอินเทอร์เน็ตปัจจุบันมีความรุนแรงและขยายตัวไปอย่างรวดเร็ว ซึ่งองค์กรใดก็ตามที่ไม่ เตรียมเครื่องมือหรือวิธีการไว้รองรับจะเผชิญกับความเสียหายอย่างหลีกเลี่ยงไม่ได้ สาเหตุสำคัญ ประการหนึ่งของการความเสียหายที่แผ่ขยายออกไปเป็นวงกว้างในเวลาที่รวดเร็วขึ้นเนื่องจาก ปัจจุบันมีผู้นิยมเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตแบบความเร็วสูง (Broadband) ทำให้ปริมาณข้อมูล ที่วิ่งบนเครือข่ายอินเทอร์เน็ตมีจำนวนเพิ่มมากขึ้น ตัวอย่างความเสียหายที่รู้จักกันดีคือไวรัส คอมพิวเตอร์ประเภทหนอนอินเทอร์เน็ต (Worm) ที่สามารถแพร่กระจายผ่านจดหมาย อิเล็กทรอนิกส์ (E-mail) ได้อย่างรวดเร็วอาทิเช่น Code Red, NIMDA, SQL Slammer, MSBlaster, และ Sasser worm ซึ่งได้สร้างความเสียหายต่อองค์กรหลายแห่งอย่างมากมาย

2.2 หลักการพื้นฐานของระบบรักษาความปลอดภัยข้อมูล

Ronald L. Krutz (2001) องค์ประกอบที่สำคัญ สามประการของการรักษาความ ปลอดภัยของข้อมูลคือ C.I.A ได้แก่ การรักษาให้เป็นความลับ (Confidentiality) การคงความ สมบูรณ์ (Integrity) และความพร้อมเมื่อต้องการใช้งาน (Availability)

การรักษาให้เป็นความลับ หมายถึง ความพยายามในการปกป้องข้อมูล จากความไม่ตั้งใจ(ของผู้ที่ได้รับสิทธิ์) หรือ จากความตั้งใจ (จากผู้ที่ไม่ได้รับสิทธิ์) ในการเปิดเผยข้อมูลภายในขององค์กร

ความคงสมบูรณ์ หมายถึงข้อมูลต้องคงความถูกต้องอยู่เสมอ ประกอบไปด้วย

1. การเปลี่ยนแปลงจะต้องมาจากผู้ที่ได้รับอนุญาต
2. การเปลี่ยนแปลงอย่างไม่ตั้งใจจะต้องไม่เกิดจากผู้ที่ได้รับอนุญาต
3. ข้อมูลที่มีความสัมพันธ์กัน จะต้องดำรงความสัมพันธ์กันอยู่อย่างสมเหตุสมผล เช่น ยอดรวมรายรับ ต้องเท่ากับ ยอดรายรับย่อยรวมกัน

ความพร้อมเมื่อต้องการใช้งาน หมายถึงเสถียรภาพของระบบและระยะเวลาในการใช้งานระบบต้องมีความน่าเชื่อถือ เมื่อมีความต้องการใช้งานระบบ ระบบจะต้องสามารถตอบสนองได้ทันที

องค์กรใดก็ตามที่ต้องการให้เกิด C.I.A จะต้องพยายามหาทางป้องกัน D.A.D ได้แก่ Disclosure , Alteration , Destruction หมายถึง

1. การเปิดเผยข้อมูลที่เป็นความลับ
2. การเปลี่ยนแปลงแก้ไขข้อมูล (ทั้งจากความตั้งใจและไม่ตั้งใจ)
3. การทำลายระบบ

และนอกเหนือจากองค์ประกอบทั้งสามประการที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัย โดยเฉพาะอย่างยิ่งในระบบเครือข่ายนั้น ยังมีองค์ประกอบด้านอื่นที่จะต้องพิจารณาร่วมด้วยได้แก่ Identification, Authentication , Accountability, Authorization, Privacy

Identification หมายถึงความสามารถในการระบุตัวตนของผู้ที่เข้ามาใช้งานระบบ ซึ่งการระบุตัวตนนี้จะมีความสัมพันธ์กับการให้สิทธิ์ของผู้ที่เข้ามาใช้งานระบบ ดังนั้นวิธีการที่จะระบุว่าบุคคลใดจะสามารถเข้าไปใช้งานระบบได้บ้างนั้นสามารถทำได้หลายวิธี เช่นใช้การใช้ รหัสผ่าน การใช้ บัตร หรือการใช้ลายนิ้วมือ

Authentication หมายถึง ขั้นตอนในการการระบุตัวตนของผู้ที่เข้ามาใช้งานระบบโดยในขั้นตอนนี้ระบบจะต้องทำการตรวจสอบเพื่อให้แน่ใจว่าผู้ที่เข้ามาใช้งานระบบนั้นคือบุคคลผู้นั้นอย่างแท้จริงไม่ได้มีการปลอมตัวมา ตัวอย่างวิธีการได้แก่ การใช้รหัสผ่าน การใช้บัตรสมาร์ทการ์ด หรือการใช้ลายนิ้วมือพิสูจน์ เป็นต้น

Accountability หมายถึง ความสามารถของระบบในการติดตามพฤติกรรมการใช้งานขอผู้ใช้งานที่มีบัญชีรายชื่ออยู่ในระบบ เพื่อใช้สำหรับในการตรวจสอบและเก็บสถิติการใช้งานว่ามีแนวโน้มในการใช้งานที่เป็นภัยคุกคามต่อระบบหรือไม่

Authorization หมายถึง ขั้นตอนการกำหนดสิทธิ์และขอบเขตการใช้งานระบบของผู้ที่เข้ามาใช้ระบบ

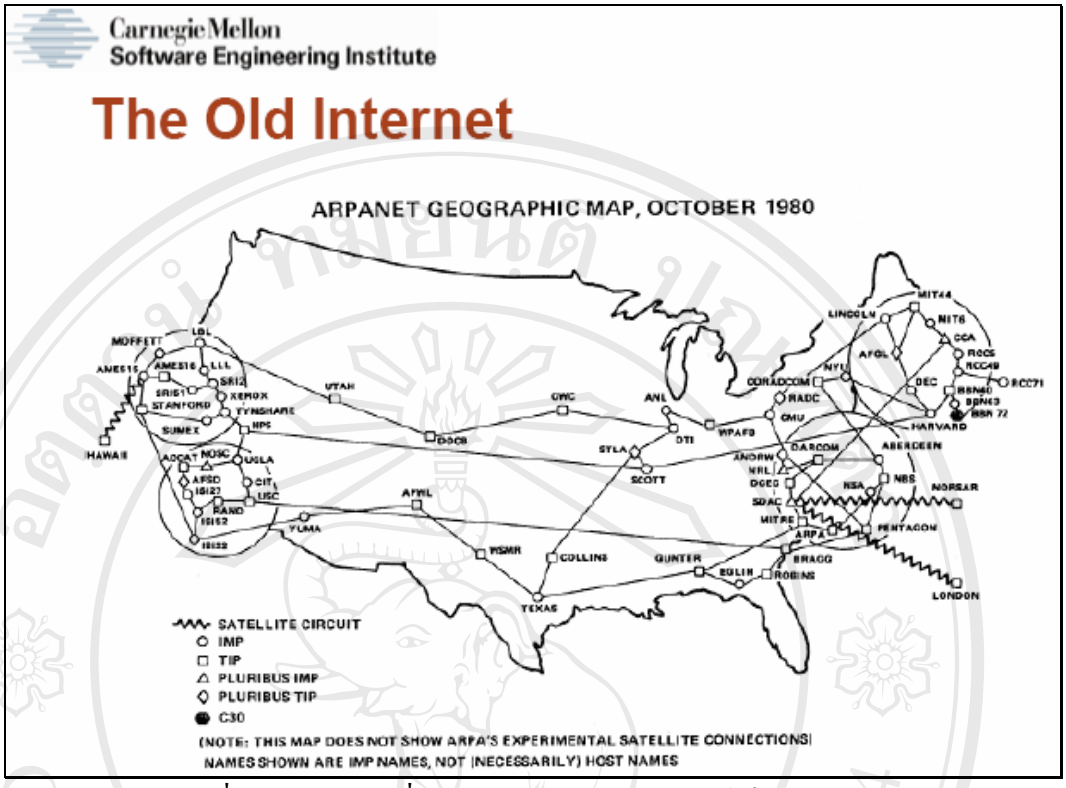
นอกจากขั้นตอนต่างๆ เหล่านี้ที่เป็นองค์ประกอบพื้นฐานของการรักษาความปลอดภัยแล้ว สิ่งสำคัญอีกประการหนึ่งที่ทุกองค์กรควรมี นั่นคือนโยบายการใช้งาน ซึ่งควรแบ่งประเภทและระดับการใช้งานให้ชัดเจน จะช่วยเพิ่มในเรื่องของการควบคุมการใช้งานให้เป็นไปในทิศทางที่กำหนดไว้ได้อย่างถูกต้องมากยิ่งขึ้น

2.3 กำเนิดของเครือข่ายอินเทอร์เน็ต

อินเทอร์เน็ตเป็นเทคโนโลยีสารสนเทศที่ถือกำเนิดเมื่อประมาณ 36 ปีที่แล้วในประเทศสหรัฐอเมริกา เมื่อ พ.ศ. 2512 โดยองค์กรทางทหารของสหรัฐอเมริกา ชื่อว่า ยูเอสดีเฟนซ์ดีพาร์ทเมนท์ (U.S.Defence Department) เป็นผู้คิดค้นระบบขึ้นมา มีวัตถุประสงค์ คือ เพื่อให้มีระบบเครือข่ายที่ไม่มีวันตายแม้จะมีสงคราม ระบบ การสื่อสารถูกทำลาย หรือตัดขาด แต่ระบบเครือข่ายแบบนี้ยังทำงานได้ ซึ่งระบบดังกล่าวจะใช้วิธีการส่งข้อมูลในรูป ของคลื่นไมโครเวฟ ฝ่ายวิจัยขององค์กรจึงได้จัดตั้งระบบเน็ตเวิร์กขึ้นมา เรียกว่า Arpanet ย่อมาจากคำว่า Advance Research Project Agency network ซึ่งประสบความสำเร็จและได้รับความนิยมในหมู่ของหน่วยงานทหาร องค์กรรัฐบาล และสถาบันการศึกษาต่างๆ เป็นอย่างมาก

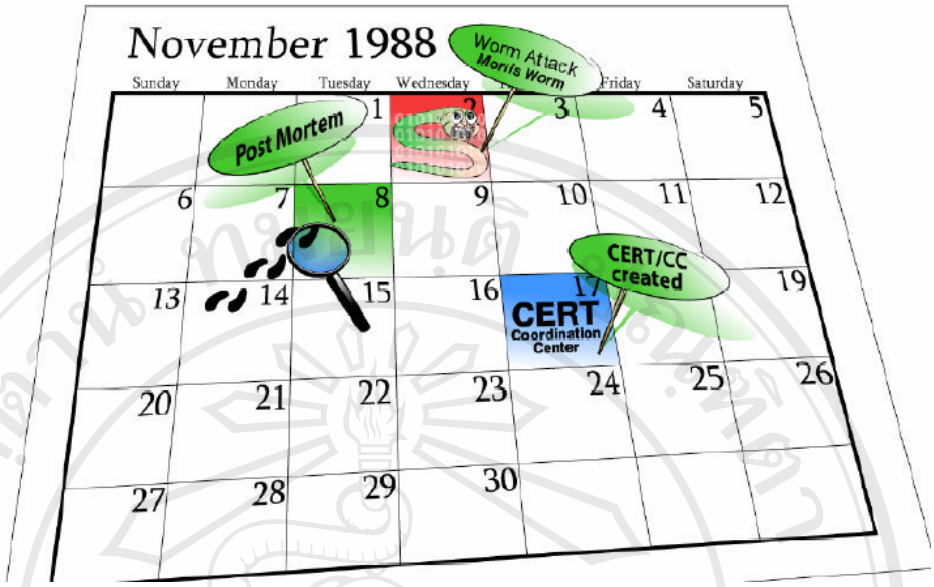
ARPANET protocols (กฎเกณฑ์ในการสื่อสารบนเครือข่ายคอมพิวเตอร์) ในตอนแรกนั้นได้ถูกออกแบบบนพื้นฐานของระบบแบบเปิดและมีความยืดหยุ่นแต่ไม่ได้คำนึงในแง่ของความปลอดภัย นักวิจัยที่สร้างมันเพื่อต้องการเพียงแค่ความง่ายในการแบ่งปันข้อมูล ดังนั้นจึงมิได้จำกัดการใช้งานใดๆ ของผู้ที่อยู่ในเครือข่าย อย่างไรก็ตามแนวทางที่วางเอาไว้ในตอนนั้นคงไม่เหมาะสมกับการใช้งานอินเทอร์เน็ตในทุกวันนี้

เริ่มมีการเชื่อมต่อเข้าสู่เครือข่าย ARPANET มากขึ้น โดยเครื่องที่อยู่ในเครือข่ายส่วนใหญ่จะเป็นของมหาวิทยาลัยและหน่วยงานต่างๆ ของรัฐบาล และแอพลิเคชั่นที่ใช้งานในตอนนั้นยังเป็นแบบพื้นฐานในการสื่อสารทั่วๆ ไปเช่น จดหมายอิเล็กทรอนิกส์ (E-mail), กลุ่มข่าวสารอิเล็กทรอนิกส์ (newsgroup), และการเชื่อมต่อคอมพิวเตอร์ในระยะทางไกล โดยในปี 1971 มีการเชื่อมต่อประมาณ 24 เครือข่ายเข้าหากันทั้งจากของรัฐบาลและมหาวิทยาลัย โดยเฉพาะอย่างยิ่งนักวิจัยในมหาวิทยาลัยจะใช้ประโยชน์ในแง่ของการแลกเปลี่ยนข้อมูลข่าวสาร ซึ่ง ARPANET ได้เริ่มกลายเป็นเครื่องมือชิ้นสำคัญในการทำงานวิจัย



รูปที่ 2.1 แสดงการเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ตในยุคแรก

ในปี 1986 ได้มีการรายงานเกี่ยวกับการละเมิดความปลอดภัยเป็นครั้งแรกโดย Cliff Stoll แห่งห้องปฏิบัติการแห่งชาติ ลอเรนต์ (Lawrence Berkeley National Laboratory) ของ Berkeley ใน California ตอนเหนือ โดย Stoll พบว่ามีความพยายามที่จะเชื่อมต่อเข้ามาในเครือข่าย ARPANET เพื่อทำการคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์ในเครือข่ายจากบัญชีผู้ใช้ที่ไม่ได้อยู่ในระบบ ซึ่งหลังจากที่ได้รายงานข้อผิดปกตินี้ออกไป เริ่มมีความกังวลว่าอาจจะเริ่มมีการใช้งาน ARPANET ในทางประสงค์ร้ายในอนาคต

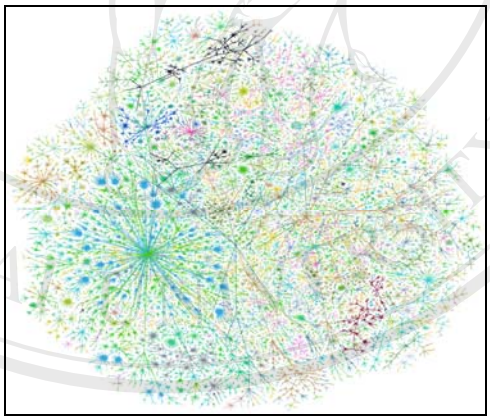


รูปที่ 2.2 แสดงลำดับเหตุการณ์ที่เกี่ยวข้องกับเรื่องความปลอดภัยในเครือข่ายอินเทอร์เน็ตปี 1988

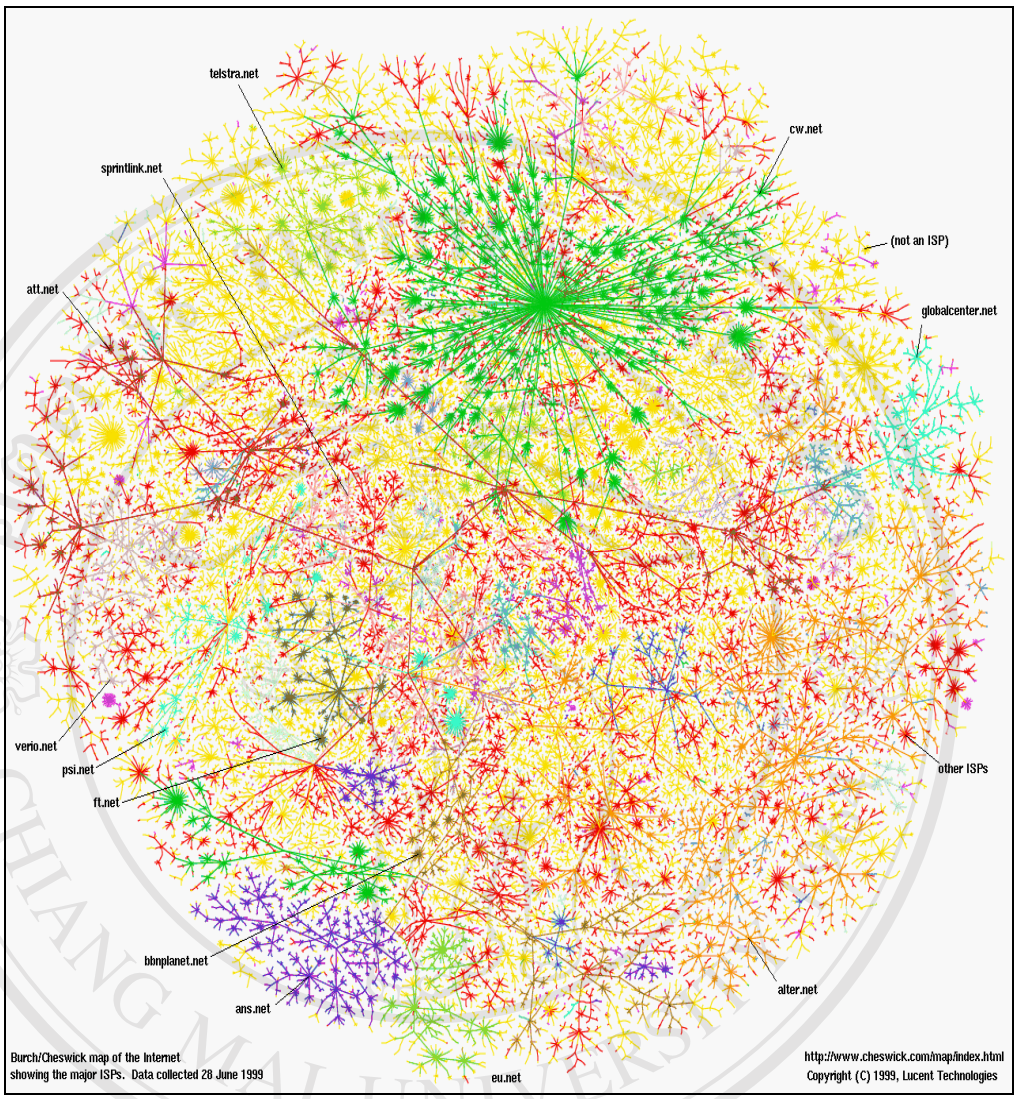
ในปี 1988 ARPANET ได้เผชิญกับปัญหาในด้านความปลอดภัยที่สามารถทำงานได้อย่างอัตโนมัติเป็นครั้งแรก ซึ่งเกิดจากการเขียนโปรแกรมของนักศึกษาที่มหาวิทยาลัยคอร์เนลชื่อ Robert T Morris ซึ่งเรียกโปรแกรมนั้นว่าหนอน (Worm) สิ่งที่โปรแกรมหนอนทำคือการค้นหาเส้นทางและใช้ช่องโหว่ของระบบในการคัดลอกตัวหนอนไปยังเครื่องอื่นๆ ในเครือข่ายไปเรื่อยๆ การทำเช่นนี้ทำให้มีการใช้ทรัพยากรของระบบจำนวนมาก ดั้งนั้นคอมพิวเตอร์ประมาณ 10% ที่เชื่อมต่ออยู่ในเครือข่าย ARPANET จึงหยุดการทำงานในเวลาเดียวกัน โดยในขณะนั้นมีคอมพิวเตอร์มากกว่า 88,000 เครื่องทำการเชื่อมต่ออยู่ในระบบ หลายแห่งไม่สามารถรับมือกับหนอนได้จึงทำการยกเลิกการเชื่อมต่อกับเครือข่าย ARPANET ออกไปเป็นจำนวนมาก หนอน Morris ทำให้ Defense Advanced Research Projects Agency (DARPA, ชื่อใหม่ของ ARPA) ได้ระดมทุนเพื่อสร้างทีมงานในการตอบสนองต่อภาวะฉุกเฉินคอมพิวเตอร์ ซึ่งก็คือ CERT (Computer Emergency Response Team)ในปัจจุบัน เพื่อให้มีศูนย์รวมของผู้เชี่ยวชาญด้านความปลอดภัยสำหรับทำงานในภาวะฉุกเฉินที่เกิดขึ้นกับเครือข่าย และ CERT เองได้ตั้งหน่วยงานอย่างไม่เป็นทางการขึ้นมาเพื่อช่วยกันรับมือสถานการณ์ฉุกเฉินด้วยคือ Forum of Incident Response and

Security Teams (FIRST). โดยทั้งสองหน่วยงานนี้จะทำงานประสานกันในการรับมือกับภัยคุกคามต่อระบบ

ในปี 1989 เครือข่าย ARPANET ได้กลายมาเป็น Internet อย่างเป็นทางการและมีคอมพิวเตอร์ที่ทำการเชื่อมต่อเข้าสู่เครือข่ายมากกว่า 100,000 เครื่อง ส่วนปัญหาเรื่องความปลอดภัยก็ยังมีอยู่ โดยเหมือนจะเริ่มเป็นการเผชิญหน้ากันของสองเทคโนโลยีคือ ด้านที่เกี่ยวกับการรุกรานและด้านที่จะหาทางป้องกัน ซึ่งในปี 1989 นี้เองที่มีการปรากฏตัวของโปรแกรมหนอนที่ชื่อว่า WANK/OILZ โดยตัวหนอนทำการโจมตีระบบ VMS (ระบบปฏิบัติของบริษัท ดิจิตอลอิคิวเมนต์) ซึ่งเชื่อมต่ออยู่ในเครือข่ายอินเทอร์เน็ต โดยทำการสำรวจเพื่อหาช่องโหว่ของระบบจากโปรแกรม send mail (โปรแกรมสำหรับรับส่งจดหมายอิเล็กทรอนิกส์) ในปี 1994 ได้มีการสร้างเครื่องมือสำหรับการโจมตีขึ้นมาเพื่อทำการดักจับ (sniff) ข้อมูลในเครือข่าย ซึ่งทำให้สามารถล่วงรู้ทั้งบัญชีรายชื่อและรหัสผ่านของผู้ใช้ระบบในขณะนั้นได้



รูปที่ 2.3 แสดงโครงสร้างของอินเทอร์เน็ตในวันที่ 16 สิงหาคม 2541



รูปที่ 2.4 แสดงการเชื่อมโยงในเครือข่ายอินเทอร์เน็ตปัจจุบัน

จากวัตถุประสงค์ในตอนแรกเป็นโครงการของรัฐบาลเพื่อใช้ในการค้นคว้าและวิจัย ได้เปลี่ยนรูปแบบไปเป็นแหล่งในการติดต่อสื่อสาร การทำธุรกรรม การค้า ความบันเทิงหลายหลายรูปแบบ ซึ่งแน่นอนว่าปัญหาในเรื่องของรูปแบบการความเสียหายต่าง ๆ จากอินเทอร์เน็ตก็ได้มีวิวัฒนาการที่เปลี่ยนไปด้วย

2.4 ประเด็นที่เกี่ยวข้องกับเรื่องของความปลอดภัยและประเภทของการละเมิดบนเครือข่าย

เหตุการณ์ที่เกี่ยวข้องกับเรื่องของความปลอดภัยในระบบเครือข่ายมักจะเกี่ยวข้องกับกิจกรรมที่ก่อให้เกิดผลในทางลบต่อระบบ โดยทั่วไปแล้วมักจะเป็นเรื่องของการละเมิดนโยบายในด้านการรักษาความปลอดภัยที่ได้กำหนดไว้แล้วขององค์กร ซึ่งอาจเกิดจากคนในองค์กร หรือมาจากเครือข่ายภายนอกองค์กรอย่างเช่น อินเทอร์เน็ต การโจมตีบางครั้งมุ่งไปที่ระบบบางระบบโดยเฉพาะ และบางครั้งก็ต้องอาศัยบัญชีรายชื่อพิเศษจากระบบ เช่น ของผู้ดูแลระบบนั้นๆ

ซึ่งรูปแบบในการโจมตีบางครั้ง มุ่งไปที่บัญชีรายชื่อบางอันของระบบ หรือของผู้ดูแลระบบเพื่อให้ได้สิทธิ์ในการจัดการกับระบบ หรืออาจใช้ระบบที่ได้ตกเป็นเหยื่อแล้วเพื่อมุ่งโจมตีไปยังระบบอื่นๆ โดยทั่วไปสามารถทำได้ในเวลาแค่ 45 วินาที ซึ่งในอนาคตอาจทำได้เร็วขึ้นกว่านี้อีก

แหล่งที่มักจะเข้าโจมตีระบบ บางครั้งการจะระบุว่าเป็นใครที่เข้ามาบุกรุกระบบค่อนข้างทำได้ยาก พวกเค้าเหล่านั้นอาจเป็นนักศึกษาที่อยากรู้อยากเห็น โดยใช้อินเทอร์เน็ตเป็นเครื่องมือ หรืออาจเป็นบุคคลที่ต้องการข้อมูลเพื่อเป็นประโยชน์ต่อการแข่งขันในด้านธุรกิจ หรืออาจเป็นพนักงานภายในองค์กรนั้นๆ เอง โดยส่วนใหญ่แล้วมักจะโจมตีจากช่องโหว่หรือช่องโหว่จากการปรับแต่งระบบที่ผิดพลาด ผู้บุกรุกที่ประสบความสำเร็จในการโจมตีระบบหลายๆ ครั้งจะยิ่งสร้างความเสียหายเพิ่มมากขึ้นเรื่อยๆในครั้งถัดไป

เหตุการณ์ที่ใช้ในการโจมตี สามารถแบ่งเป็นประเภทต่างๆได้ดังต่อไปนี้ probe, scan, account compromise, root compromise, packet sniffer, denial of service, exploitation of trust, malicious code, และ Internet infrastructure attacks.

Probe (โพรบ) เป็นลักษณะของการทดลองหรือการเดาวิธีการหรือแนวทางเพื่อหาทางเข้าสู่ระบบ ตัวอย่างเช่นมีการ พยายามเข้าสู่ระบบ จากบัญชีรายชื่อที่ไม่ได้ใช้ หรือ จากการเดาบัญชีรายชื่อที่มีอยู่ในระบบ ดังนั้นหากบัญชีผู้ใช้ในระบบมีการการกำหนดรหัสผ่านที่ง่ายต่อการเดาด้วยวิธีการ probe จะทำให้ผู้ที่โจมตีสามารถใช้ช่องโหว่นี้เข้าทำลายระบบได้ง่าย

Scan (สแกน) เป็นลักษณะของวิธีการ โพรบด้วยจำนวนความถี่หรือจำนวนครั้งมากๆ ซึ่งบางครั้งจะได้ผลลัพธ์ที่เป็นประโยชน์ในการที่จะใช้ในการโจมตีระบบต่อไป ยกตัวอย่างเช่น การทดลองสุ่มใช้รหัสผ่านจำนวนหนึ่งกับบัญชีรายชื่อผู้ใช้ในระบบ โดยรหัสผ่านที่ใช้จะเป็นรหัสผ่านที่มักเป็นที่นิยมสำหรับผู้ใช้ทั่วไปที่ไม่ได้ใส่ใจกับเรื่องของความปลอดภัยของระบบ

Account Compromise (การแอบเข้าไปใช้งานระบบจากบัญชีผู้ใช้คนอื่น) เป็นลักษณะเข้าไปใช้งานจากระบบโดยที่ใช้บัญชีรายชื่อของบุคคลอื่นที่อยู่ในระบบ เพื่อทำการขโมยข้อมูลหรือทำลายข้อมูล และหากผู้ใช้ที่เป็นผู้ดูแลระบบขาดความใส่ใจในเรื่องของความปลอดภัย อาจ

นำไปสู่ปัญหาเรื่องความปลอดภัยในระดับที่รุนแรงขึ้น

Root Compromise (การแอบเข้าไปใช้งานระบบจากบัญชีผู้ใช้ในระดับผู้ดูแลระบบ) มีลักษณะเหมือนกับ Account compromise แต่ระดับสิทธิ์ที่ได้มีมากกว่ากล่าวคือ ผู้บุกรุกสามารถทำได้ทุกอย่างที่ผู้ดูแลระบบปกติทำได้ ซึ่งสามารถสร้างความเสียหายได้อย่างร้ายมาก

Packet Sniffer (การดักจับข้อมูล) เป็นลักษณะของการบุกรุกโดยอาศัยโปรแกรมที่มีความสามารถในการดักจับข้อมูลที่ถูกส่งผ่านไปมาในระบบเครือข่าย ซึ่งข้อมูลเหล่านั้นอาจประกอบไปด้วย บัญชีรายชื่อที่อยู่ในระบบและรหัสผ่าน ซึ่งโดยมากข้อมูลในระบบมักจะเป็นข้อความธรรมดาที่ไม่ได้ทำการเข้ารหัสไว้

Denial of Service (การทำให้หยุดบริการ) วัตถุประสงค์ของการโจมตีในลักษณะของการให้ระบบเป้าหมายหยุดให้บริการ ต่างจากการจู่โจมแบบอื่นคือ ไม่ได้มุ่งหวังในการเข้าไปใช้งานระบบ แต่ต้องการให้ระบบนั้นหยุดทำงาน วิธีการโจมตีเพื่อให้หยุดการให้บริการสามารถทำได้หลายรูปแบบ เช่น การทำ “flood” เพื่อทำให้เครื่องเป้าหมายได้รับข้อมูลเป็นปริมาณมากๆ จนไม่สามารถตอบสนองต่อการให้บริการได้ทันจนในที่สุดหยุดให้บริการไป ความเสียหายจากการทำให้เกิดการหยุดให้บริการนั้นขึ้นอยู่กับหน้าที่ของระบบนั้นๆ ว่ามีความสำคัญอย่างไร เช่นถ้าระบบนั้นต้องรองรับการให้บริการการทำธุรกรรมผ่านทางอินเทอร์เน็ต มูลค่าความเสียหายก็จะมากกว่าระบบที่ให้บริการข่าวสารทั่วๆไป

Exploitation of Trust (การอาศัยช่องโหว่จากความเชื่อถือจากเครื่องที่ใช้งานร่วมกัน) การสื่อสารระหว่างคอมพิวเตอร์ที่อยู่ในเครือข่ายที่อาศัยความเชื่อถือกันว่าถ้าเป็นเครื่องที่ตกลงกันไว้เข้ามาขอใช้งานระบบ ก็จะอนุญาตให้ดำเนินการได้ แต่ผู้บุกรุกสามารถปลอมแปลงเครื่องให้มีคุณลักษณะที่เป็นเครื่องที่ได้สร้างข้อตกลงกันไว้เพื่อแอบเข้าไปใช้งานในระบบได้

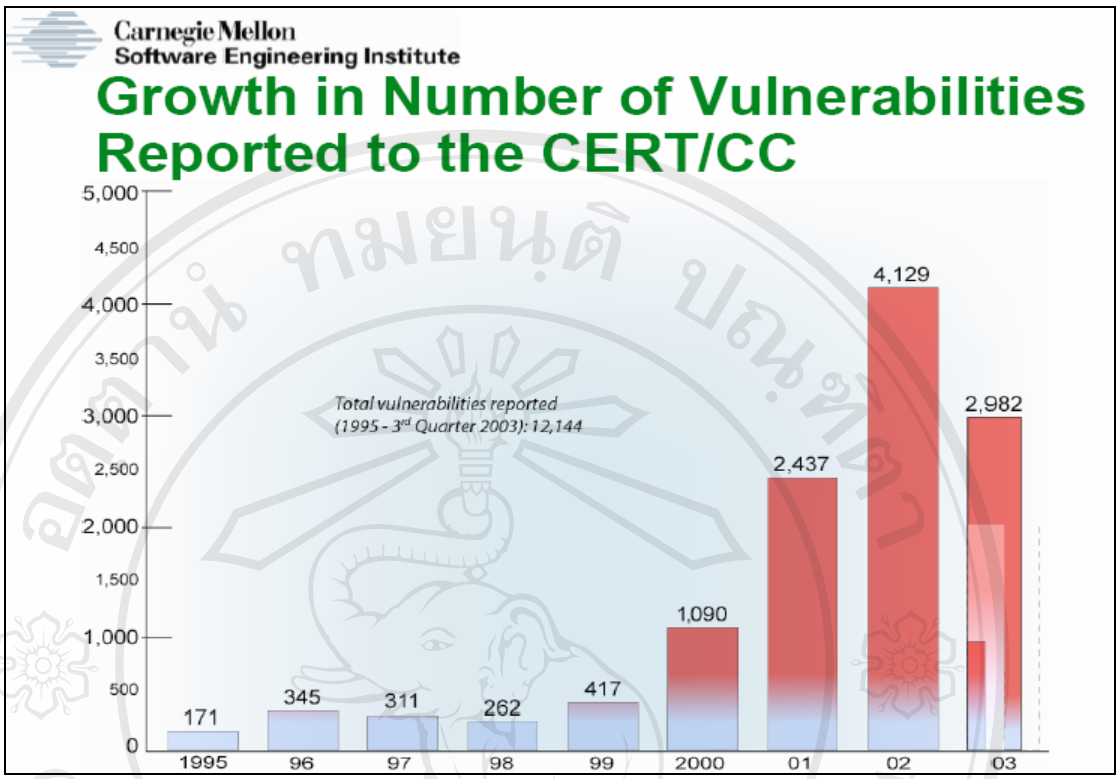
Malicious Code (โปรแกรมที่ประสงค์ร้าย) มักจะเป็นโปรแกรมที่เราไม่อาจคาดเดาผลลัพธ์ที่ได้จากการใช้งานบนระบบ ผู้ใช้งานโดยทั่วไปแล้วไม่ได้มีความระมัดระวังเกี่ยวกับการใช้งานโปรแกรมเท่าที่ควรบางครั้งสั่งให้โปรแกรมที่ไม่รู้จักทำงานและกว่าจะพบว่าเป็นโปรแกรมที่มุ่งประสงค์ร้ายก็มักจะเกิดความเสียหายขึ้นแล้ว โปรแกรมที่ประสงค์ร้ายประกอบไปด้วย โปรแกรมแบบม้าโทรจัน (Trojan horses) โปรแกรมไวรัส (Viruses) โปรแกรมหนอน (Worms) โปรแกรมแบบม้าโทรจันและไวรัสส่วนมากจะทำการซ่อนตัวเองอยู่ในโปรแกรมอื่นๆ อีกทีหนึ่ง หรืออาจเป็นไฟล์ที่ผู้โจมตีได้เปลี่ยนแปลงแก้ไขการทำงานภายในเรียบร้อยแล้ว โปรแกรมหนอนเป็นโปรแกรมที่สามารถทำงานได้ด้วยตัวเองจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งในระบบเครือข่าย โดยไม่ต้องอาศัยให้ผู้ใช้ระบบเป็นคนสั่งเหมือน โปรแกรมไวรัสหรือม้าโทรจัน โปรแกรมทั้งหมดเหล่านี้

สามารถสร้างความเสียหายให้เกิดขึ้นเป็นอย่างมาก เช่นมีการสูญเสียข้อมูล เกิดการหยุดให้บริการ เป็นต้น

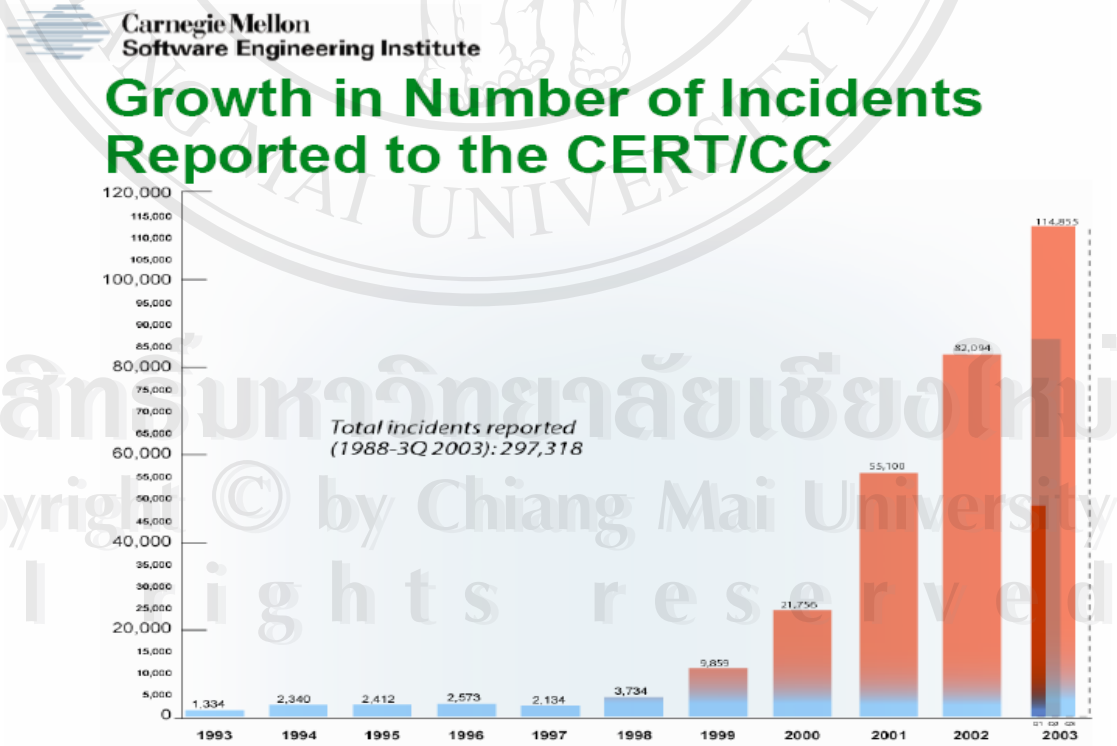
Internet Infrastructure Attacks (การโจมตีโครงสร้างพื้นฐานที่ต้องใช้ในระบบเครือข่าย) เป็นการมุ่งโจมตีไปยังระบบหลักที่เครือข่ายต้องใช้งานเช่น Name Server (เครื่องแม่ข่ายที่ทำหน้าที่เปลี่ยนชื่อเป็นไอพีแอดเดรส) เพื่อทำให้เครื่องในเครือข่ายไม่สามารถใช้งานอินเทอร์เน็ตหรือมุ่งไปที่เครื่องที่ทำหน้าที่เป็นเกตเวย์ (Gateway) เพื่อหยุดการให้บริการ การโจมตีลักษณะนี้เกิดได้ค่อนข้างยาก แต่เมื่อเกิดแล้วจะทำให้ระบบหยุดทำงานเป็นเวลานาน

2.5 แนวโน้มการบุกรุกบนระบบเครือข่ายคอมพิวเตอร์ในอนาคต

ช่วงระหว่างปี 1980 ถึง 1990 การบุกรุกเข้าไปในระบบเครือข่ายยังเป็นวิธีแบบที่ไม่ซับซ้อน เช่นการเดาจากรหัสผ่านที่ตั้งกันง่ายเกินไปหรือการมุ่งโจมตีจากข้อผิดพลาดในการปรับแต่งระบบของผู้ดูแลระบบเป็นหลัก เพื่อให้สามารถเข้าไปใช้งานระบบ วิธีการเช่นนี้ยังคงมีประสิทธิอยู่ในการจะเข้าไปเจาะระบบใดระบบหนึ่ง ไม่ว่าระบบนั้นได้สร้างมาให้มีความปลอดภัยแค่ไหนก็ตาม แต่หากผู้ดูแลระบบละเลยความเอาใจใส่ย่อมเป็นช่องโหว่ได้ตลอดเวลา การโจมตีประเภทนี้ยังคงทำกันมาเรื่อยจนกระทั่งในปี 1996 เริ่มมีวิธีการที่ซับซ้อนเพิ่มมากขึ้นในหมู่ผู้บุกรุกระบบทั้งหลาย มีการพัฒนาวิธีการใหม่ในการโจมตีและมีการแลกเปลี่ยนความรู้ในการโจมตีระบบซึ่งกันและกัน โดยบางกลุ่มได้สร้างเครื่องมือที่จะสามารถโจมตีได้อย่างอัตโนมัติขึ้น และในขณะเดียวกันก็มีการพัฒนาองค์ความรู้ของการโจมตีให้มีมากขึ้นด้วย



รูปที่ 2.5 แสดงรายงานเรื่องจำนวนช่องโหว่ต่างๆ ที่ค้นพบในช่วงปี 1995-2003



รูปที่ 2.6 แสดงจำนวนเหตุการณ์การเกี่ยวเรื่องความปลอดภัยในเครือข่ายอินเทอร์เน็ต

ปริญญา หอมเอนก (2547) ได้กล่าวถึงแนวโน้มของด้านความปลอดภัยของเทคโนโลยีสารสนเทศ ดังนี้

1. Wireless Hacking : "War Driving and War Chalking"

การเจาะระบบเครือข่ายไร้สายไม่ว่าจะเป็น Wi-Fi (IEEE 802.11b) หรือ มาตรฐานใหม่ที่กำลังเป็นที่นิยมคือ IEEE 802.11g ที่เร็วกว่าเดิม ล้วนตกเป็นเป้าหมายของ Hacker ในยุคนี้ ซึ่งจะมีศัพท์เฉพาะในการเจาะระบบไร้สาย ที่ควรทราบได้แก่คำว่า "War Driving" และ "War Chalking"

War Driving หมายถึง การที่เหล่า Hacker ใช้วิธีขับรถตระเวนไปตามย่านธุรกิจ ที่คาดว่าจะมีการใช้งาน Access Point[1] ที่ให้บริการอินเทอร์เน็ตแบบไร้สายแล้วพยายาม "HACK" เพื่อที่จะได้เล่นอินเทอร์เน็ตฟรี หรือเข้าสู่ระบบของบุคคลอื่นโดยไม่ได้รับอนุญาต เป็นต้น

ส่วน War chalking หมายถึง การที่เหล่า Hacker ทำการกำหนดตำแหน่งของจุดให้บริการเครือข่ายไร้สายที่เปิดให้ใช้บริการแบบสาธารณะ เพื่อที่จะเป็นข้อมูลให้ Hacker กลุ่มอื่น ๆ ได้ทราบและนำข้อมูลนี้มาใช้ในการ On-Line เข้าสู่ระบบเครือข่ายไร้สายของบุคคลอื่นได้ง่ายยิ่งขึ้น ดูตัวอย่างที่ www.wigle.net

2. IPS (Intrusion Prevention System) : "Next Generation IDS (Intrusion Detection System)"

IPS (Intrusion Prevention System) เป็นเทคโนโลยีใหม่ที่คาดว่าจะมาแทน IDS (Intrusion Detection System) โดยที่ IPS จะสามารถป้องกันและหยุดการจู่โจมของ Hacker ได้ ขณะที่ IDS ได้แต่เพียงทำการเตือนเวลามีผู้บุกรุกเท่านั้น (ยกเว้น IDS ที่มีคุณสมบัติในการ "Reset" การต่อเชื่อมไม่พึงประสงค์จากภายนอกเข้าสู่ระบบ)

IPSดูเหมือนจะเป็นเทคโนโลยีที่มีอนาคตเพราะสามารถหยุดการจู่โจมของ Hacker โดยเฉพาะแบบ DoS (Denial Of Services) Attack รวมถึง Virus หรือ Worm ใหม่ ๆ ที่คาดว่าจะเกิดขึ้นอีกในอนาคตอันใกล้ แต่ข้อเสียของ IPS คือ ยังเป็นเทคโนโลยีใหม่ที่ต้องมีการพิสูจน์ว่าจะได้ผลจริงหรือไม่ และ IPS อาจจะทำงานผิดพลาดโดยทำการหยุด Traffic ของระบบเครือข่ายที่เป็น Traffic ปกติทั่วไป (ไม่ใช่ของ Hacker) ทำให้ระบบอาจมีปัญหาเรื่องของ Availability ได้ (เกิด Downtime) ดังนั้น การใช้งาน IPS จึงต้องกำหนดจุดติดตั้งและมีการทดสอบให้ดีเสียก่อนอีกทั้ง IPS ยังมีราคาที่ค่อนข้างแพง

3. Web Server/Web Application Hacking : "Next Generation Hacking Concept for Next Generation Hacker"

---

[1] Access Point คืออุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

เนื่องจากทุกวันนี้องค์กรต่าง ๆ ที่ต่อเชื่อมกับระบบอินเทอร์เน็ตล้วนมีการใช้ Firewall ในการป้องกันระบบของตนเองโดย Firewall จะเปิดให้บริการเฉพาะ port 80 (http) และ port 443 (https) เท่านั้น Hacker จึงต้องพยายามหาวิธีในการเจาะเข้าระบบโดยผ่านทางช่องทางที่เปิดอยู่แล้วนั้นคือทาง Web Application[2] นั่นเอง ไม่ว่าจะเขียนด้วย ASP, PHP หรอ JSP ก็ล้วนมีช่องโหว่ที่ Hacker อาจที่จะเจาะเข้ามาได้จากการเขียน Web Application แบบไม่ระมัดระวัง การใช้งานโปรแกรมประเภท CMS (Content Management System) เช่น phpNuke หรือ phpBB ก็มีช่องโหว่ให้ Hacker โจมตี เช่นกัน

เพราะฉะนั้น องค์กรต่างๆจึงควรมีการฝึกอบรมเรื่องความตื่นตัวหรือความระมัดระวังในการใช้งานเทคโนโลยีพร้อมทั้งตระหนักในเรื่องของการรักษาความปลอดภัย โปรแกรมเมอร์ผู้พัฒนาระบบ เพื่อให้มีความเข้าใจเรื่องวิธีการเขียน Web Application อย่างปลอดภัยจากการจู่โจมของ Hacker และหมั่นคอยติดตามลง "Patch"[3] ให้กับ CMS ที่เราใช้งานอยู่ตลอดจน Web Sever ที่ใช้ประจำ เช่น Apache และ Microsoft IIS เป็นต้น

4. Computer Forensics and ICT Computer Laws : "Hacking in Thailand incidents are on the rise"

ในปัจจุบันการเจาะระบบของ Hacker ในประเทศไทยมีแนวโน้มที่สูงขึ้นเรื่อย ๆ ทางภาครัฐจึงได้ดำเนินการออกกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้น (ดูรายละเอียดเพิ่มเติมที่ http://www.ictlaw.thaigov.net) เพื่อให้สามารถที่จะจับกุม Hacker ได้อย่างรวดเร็วและทันต่อเหตุการณ์โดยทางตำรวจหรือผู้มีอำนาจในการจับกุม และเก็บหลักฐานต้องมีความรู้ ด้านนิติคอมพิวเตอร์ (Computer Forensic) อย่างลึกซึ้งจึงจะสามารถพิสูจน์หลักฐานได้อย่างถูกต้องหมายถึง ไม่มีการจับผิดตัว หรือ จับผู้ที่ไม่ได้เป็น Hacker แต่ถูกใส่ร้ายโดย Hacker มืออาชีพ เพราะ Hacker สามารถปลอม IP Address ที่เราเรียกว่า "IP Spoofing" หรือทำการ Scan Port Server ในระบบเครือข่าย แต่มีการตั้งค่า IP Address ของตัว Port Scanner ให้เป็นค่า IP Address ของผู้บริสุทธิ์ที่ไม่รู้เรื่องกับการโจมตีของ Hacker เลย

---

[2] Web Application คือการพัฒนาโปรแกรมที่ทำงานบนเวบไซต์เป็นหลัก อาทิเช่น เวบไซต์ที่มีการซื้อขายสินค้าหรือบริการ หรือ CMS (Contenet Management System) ที่เป็นเวบไซต์สำเร็จรูป

[3] Patch เป็นโปรแกรมขนาดเล็กทำหน้าที่ซ่อมแซมโปรแกรมที่ได้ติดตั้งไปก่อนหน้านี้แล้วและมีปัญหาเรื่องความไม่ปลอดภัย

ดังนั้น ข้อมูล Log[4] ของระบบไม่ว่าจะเป็น RADIUS Log หรือ Proxy Cache Log จึงเป็นข้อมูลที่มีความสำคัญและต้องเก็บ ไว้ระยะหนึ่งเพื่อใช้ในการตามหาแหล่งที่มาของ Hacker ว่ามาจาก IP Address ใด โดยกฎหมายควรจะออกมาครอบคลุม รายละเอียดในส่วนนี้ระดับหนึ่ง

5. The World of MalWare : "Next Year, Prepare and protect yourself from the new and intelligence Virus/Worm"

โปรแกรมจำพวก MalWare ที่มุ่งร้ายต่อระบบของเราไม่ว่าจะเป็นพวก Key logger, Trojan Horse, Ad ware, Spy Ware ต่าง ๆ ล้วนมีแนวโน้มเพิ่มมากขึ้นเรื่อย ๆ โปรแกรมเหล่านี้สามารถเข้าสู่เครื่องเรา เพียงแต่เราเข้าไปชม Web Site ที่มีการวางกับดักไว้ โดย Browser ของเราจะถูก "Hijack"[5] โดยอัตโนมัติ ทำให้โปรแกรมเหล่านี้สามารถเข้ามาฝังตัวอยู่ในเครื่องเราผ่านทาง Browser ที่มีช่องโหว่ ดังนั้นเราต้องหมั่น "Patch" Browser ขององค์กรอยู่เสมอ เพื่อไม่ให้ตกเป็นเหยื่อของ Malware

6. Managed Security Services Provider (MSSP) : "ICT Security Outsourcing Trend is coming"

การจัดการกับระบบรักษาความปลอดภัยข้อมูลคอมพิวเตอร์อย่างถูกต้องและให้ได้ผลนั้นมีรายละเอียดและต้องใช้ทรัพยาการขององค์กรค่อนข้างมากไม่ว่าจะเป็นบุคลากร งบประมาณ ในการจัดซื้อจัดจ้าง Hardware/Software ตลอดจนค่าฝึกอบรมพนักงานด้าน Information Security ดังนั้น องค์กรในยุคปัจจุบัน จึงนิยมการ "Outsourcing"[6] การดูแลรักษาความปลอดภัยข้อมูลให้กับหน่วยงานที่มีความชำนาญเฉพาะทางเรียกว่า MSSP (Managed Security Services Provider) โดยที่ MSSP มีหน้าที่ในการดูแลด้านความปลอดภัยโดยรวมของระบบ ไม่ว่าจะเป็นการการป้องกันและตรวจจับการจู่โจมของ Hacker การป้องกันและกำจัด Virus Computer เป็นต้น

7. WhiteHat Hacking / Penetration Testing : "Time to Hacking Your Own Networks/Servers"

การที่เราต้องการจะพิสูจน์ว่าระบบขององค์กรนั้นมีความแข็งแกร่งปลอดภัยจาก Hacker จริง ๆ คือ Hacker ไม่สามารถเจาะได้ง่าย ๆ วิธีการเดียวที่จะพิสูจน์ได้ก็คือ ต้องลองเจาะ

[4] Log คือการบันทึกพฤติกรรมการใช้งานภายในระบบหรือโปรแกรมใดๆ

[5] Hijack คือการเข้ายึดครองโปรแกรมใดบนเครื่องคอมพิวเตอร์เป้าหมายโดยไม่ได้รับอนุญาต

[6] Outsourcing คือการว่าจ้างบุคคลหรือองค์กรภายนอกที่เชี่ยวชาญมาทำงานอย่างใดอย่างหนึ่งให้

ระบบตัวเองดูโดยทำในลักษณะคล้าย ๆ กับการเจาะของ Hacker โดยการจ้าง "WhiteHat"[7] Hacker มาเจาะระบบขององค์กรและอธิบายวิธีการเจาะตลอดจนวิธีการป้องกันให้เราทราบ การเจาะระบบเพื่อที่จะให้ทะลุเข้ามาเอาข้อมูลที่เราต้องการป้องกัน หรือลองทำระบบขององค์กรให้ล่ม (Denial of Services) ในทางเทคนิคเราเรียกวิธีนี้ว่า "Penetration Testing" หรือ "PEN-TEST" โดยการเจาะจากอินเทอร์เน็ตเราเรียกว่า "Black-Box PEN-TEST" แต่ถ้าเจาะจากภายในระบบ LAN[8] ของเราเองเรียกว่า "White-Box PEN-TEST" การทำ PEN-TEST ที่ถูกต้องก็ควรทำทั้ง 2 แบบ ที่สำคัญผู้ที่เราจ้างมาเจาะระบบ ต้องไว้ใจได้และมีความสามารถสูงพอที่จะเจาะระบบของเราและบอกวิธีการแก้ไขให้เราป้องกันระบบได้อย่างถูกต้อง

8. In-Depth ICT Auditing : "A Very Important process for ICT Governance"

การตรวจสอบ (Audit) ระบบ ICT ขององค์กรนั้นเป็นเรื่องสำคัญที่ต้องทำทุกปี เพื่อที่จะประเมินความเสี่ยงของระบบ และ เป็นการตรวจสอบการทำงานของบุคลากร ICT ขององค์กรด้วยไปในตัว โดยการตรวจสอบควรแบ่งออกเป็น Internal Audit คือ การตรวจสอบภายในโดย Auditor ที่เป็นพนักงานขององค์กรเองแต่มีความเป็นอิสระไม่ขึ้นกับแผนกที่ดูแลเรื่อง ICT เช่น MIS department แต่จะขึ้นกับ Board of Director โดยตรง อีกส่วนหนึ่งก็คือ External Audit คือการจ้างผู้ตรวจสอบมืออาชีพ เช่น CISA (Certified Information System Auditor) [9]มาตรวจสอบระบบของเราอย่างถูกต้องตามหลักการ Audit ซึ่งทั่วโลกส่วนใหญ่ทำตามมาตรฐานของ ISACA

9. Personal Firewall : "A Must-Have on your computer"

การใช้ Personal Firewall กับเครื่อง PC หรือ Notebook ของเราเวลาที่เราต่อเชื่อมกับโลกอินเทอร์เน็ตกลายเป็น "เรื่องจำเป็น" เสียแล้ว เพราะภัยในอินเทอร์เน็ตนั้น ค่อนข้างน่ากลัว พูดง่าย ๆ ว่าถ้าเรา On-Line กับอินเทอร์เน็ตประมาณหนึ่งชั่วโมง (โดยต่อกับ ISP) อาจมีการโจมตีจาก Virus/Worm หรือ Hacker อิสระเขามายังเครื่องของเราโดย Personal Firewall จะบอกเราและเก็บ Log ไว้ให้เราตรวจสอบหาต้นต่อของผู้บุกรุก และป้องกันไม่ให้เครื่องเราถูกเจาะ จากการที่เรายังไม่มีเวลาลง Patch ให้กับเครื่องของเรา หรือ อาจลืมลง Patch ทำให้เครื่องเรายังคงมีช่องโหว่ (Vulnerability) ให้ Virus เข้ามาได้

---

[7] WhiteHat Hacker คือนักเจาะระบบที่มีคุณธรรม

[8] LAN (Local Area Network) เครือข่ายคอมพิวเตอร์ภายในองค์กร

[9] CISA (Certified Information System Auditor) ประกาศนียบัตรที่รับรองผู้ที่จะทำหน้าที่ตรวจสอบภายในทางด้านเทคโนโลยีสารสนเทศ

Personal Firewall จะช่วยป้องกันเครื่องเราในขณะที่เครื่องเรามีช่องโหว่ที่ยังไม่ได้ Patch ได้ระดับหนึ่ง ดังนั้นเราจึงมีความจำเป็นที่ต้องติดตั้ง Personal Firewall ไว้เสมอเวลา On-Line

10. Lack of Professional Information Security Certified Staff : "ICT Security moves to Professionalism"

ความต้องการ (Demand) ผู้เชี่ยวชาญด้าน Information Security นับวันยิ่งเพิ่มมาขึ้น เนื่องจากการโจมตีของ Hacker/Virus ที่มากขึ้นเป็นเวลาตามตัว ขณะที่จำนวนของผู้เชี่ยวชาญนั้น (Supply) มีจำนวนน้อยกว่าความต้องการจึงทำให้ผู้เชี่ยวชาญโดยเฉพาะที่ได้รับ Professional Certification ด้าน Information Security โดยตรง เช่น CISSP จาก ISC2, CISA จาก ISACA หรือ GIAC Certified จาก GIAC เป็นบุคลากรที่องค์กรต้องการให้ไปร่วมงานด้วยตลอดจนเงินเดือนค่อนข้างสูง และยังไม่พอกับความต้องการของแวดวง ICT Security ในทุกวันนี้ ดังนั้น "Security Professional" หรือ ผู้เชี่ยวชาญมืออาชีพด้านระบบการรักษาความปลอดภัยเป็นอาชีพที่น่าสนใจและควรสนับสนุนให้เพิ่มจำนวนมากขึ้นเพื่อศักยภาพในการพัฒนาประเทศและการป้องกันประเทศทางด้านการรักษาความปลอดภัยทางอินเทอร์เน็ตต่อไป

2.6 ช่องโหว่[10]ของอินเทอร์เน็ต (Internet Vulnerabilities)

สาเหตุที่ทำให้อินเทอร์เน็ตมีช่องโหว่

กฎเกณฑ์ที่ใช้ในการติดต่อสื่อสารในเครือข่ายซึ่งเป็นส่วนหนึ่งของโครงสร้างพื้นฐานของอินเทอร์เน็ตไม่ได้ถูกออกแบบให้มีความปลอดภัยตั้งแต่แรก ซึ่งการป้องกันภัยในเครือข่ายได้กลายเป็นปัญหาที่เผชิญในปัจจุบันและทำได้ค่อนข้างยากขึ้นเรื่อยๆ นอกจากนั้นในปัจจุบันอินเทอร์เน็ตไม่ได้เป็นเครือข่ายที่อยู่นิ่งอีกต่อไป มีการปรับเปลี่ยนทั้งวิธีการเชื่อมต่อ (Topology) และเทคโนโลยีที่เกี่ยวกับการรักษาความปลอดภัยอยู่ตลอดเวลา

และเนื่องจากกฎเกณฑ์ที่ใช้ในการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตที่ได้ออกแบบครั้งแรกนั้นเอื้อให้นักเจาะระบบสามารถทำการโจมตีได้ง่าย และยากต่อการตรวจสอบ นักเจาะระบบไม่จำเป็นต้องอยู่ในตำแหน่งทางภูมิศาสตร์ที่เดียวกับระบบที่ต้องการโจมตี นักเจาะระบบอาจอยู่ที่ใดก็ได้ในโลกที่สามารถเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ตได้

[10] ช่องโหว่คือจุดอ่อนที่เปิดโอกาสให้คนที่ไม่ได้รับอนุญาตให้เข้ามาใช้งานระบบนั้นๆ

ยังมีเครือข่ายอีกหลายแห่งที่เชื่อมต่อกับอินเทอร์เน็ตที่ขาดความใส่ใจในเรื่องระบบความปลอดภัย เช่น ผู้ดูแลระบบเหล่าจะไม่สนใจว่ามีอะไรเกิดขึ้นกับข้อมูลและระบบของตนตราบเท่าที่ระบบยังสามารถให้บริการได้ หรือ ไม่เชื่อว่าระบบของตนจะตกเป็นเป้าหมายในการบุกรุกเนื่องจากไม่ได้ให้บริการหรือเก็บข้อมูลที่สำคัญไว้ หรืออาจจะคิดว่าการป้องกันระบบของตนดีเพียงพอแล้ว ซึ่งในความเป็นจริงที่เทคโนโลยีมีการเปลี่ยนแปลง ผู้บุกรุกก็มีการพัฒนาเครื่องมือและเทคโนโลยีใหม่ๆอยู่เสมอเช่นกัน จึงยังไม่มีการป้องกันใดที่ดีที่สุดและมีประสิทธิภาพในการป้องกันได้ตลอดไป

และยังมีการส่งข้อมูลจำนวนมากบนอินเทอร์เน็ตที่ไม่ได้เข้ารหัส การรักษาความลับและความสมบูรณ์ของข้อมูลจึงเป็นเรื่องยาก ซึ่งไม่เพียงเป็นอันตรายต่อระบบที่ เกี่ยวกับการเงินหรือแม้กระทั่งเป็นอันตรายต่อกลไกการทำงานพื้นฐานของระบบด้วย เหตุผลอีกประการที่อินเทอร์เน็ตง่ายต่อการถูกบุกรุกคือการเติบโตและการใช้งานที่เพิ่มขึ้นอย่างรวดเร็ว ซึ่งมาพร้อมกับการใช้ริการต่างๆที่เพิ่มความซับซ้อนมากมายบน อินเทอร์เน็ต และที่สำคัญคือบ่อยครั้งที่บริการต่างๆเหล่านี้มักจะไม่ได้รับการออกแบบ ตั้งค่า หรือมีการดูแลด้านระบบความปลอดภัย การรีบเร่งผลิตซอฟต์แวร์ออกสู่ตลาดก็อาจเป็นเหตุให้ผู้พัฒนาโปรแกรมไม่มีเวลาเพียงพอในการทดสอบหรือตรวจหาข้อผิดพลาดที่อาจนำไปสู่การเป็นช่องโหว่ของระบบในอนาคตได้

ประกอบกับปัญหาด้านการทำธุรกิจ ผู้ค้ามักจะขายของตามความต้องการของลูกค้า คือ ง่ายต่อการใช้ บำรุงรักษาผลก็คือการทำให้ใช้งานง่ายมักไปไม่ได้กับการทำให้ระบบมีความปลอดภัย เพราะผู้ใช้ไม่ต้องการติดตั้งหรือกำหนดค่าอะไรเพิ่มเติมอีกหลังจากการติดตั้งและระบบสามารถใช้งานได้ตามความต้องการแล้ว ความง่ายมักจะแปรผกผันกับเรื่องของความปลอดภัย

ทำให้ในที่สุดแล้วการเติบโตขึ้นของอินเทอร์เน็ตได้เพิ่มความต้องการทางด้านการจัดการระบบรักษาความปลอดภัยไปด้วย ผู้เชี่ยวชาญทางด้านระบบรักษาความปลอดภัยจึงเป็นที่ต้องการสูง แต่ไม่เพียงพอต่อความต้องการของตลาด บุคลากรที่ยังขาดประสบการณ์ทางด้านนี้จึงถูกดึงขึ้นมาแทน และทำหน้าที่เปิดหน้าต่างรอให้ผู้บุกรุกตรวจพบเจอและบุกรุกเข้ามาสู่ระบบโดยไม่รู้ตัว

2.7 ขั้นตอนที่ผู้บุกรุกมักใช้ในการบุกรุกเข้าสู่ระบบคอมพิวเตอร์

ปริญญา หอมเอนก (2545) ได้แบ่งขั้นตอนหลักในการบุกรุกเข้าสู่ระบบไว้ดังนี้

2.7.1 การสำรวจหาข้อมูลเบื้องต้น (Foot printing)

ผู้บุกรุกจะเริ่มต้นขั้นตอนแรกของการบุกรุกเข้าสู่ระบบด้วยการหาข้อมูลเบื้องต้นที่จำเป็นต่อการบุกรุกในขั้นต่อไป โดยเป็นการสำรวจระบบจากภายนอก ผู้บุกรุกสามารถปลอมแปลงตนเองเพื่อไม่ให้ใครรู้ว่าตนเองเป็นใครและมีเจตนาอะไรได้ ด้วยการปลอมเป็นผู้ใช้งานทั่วไป ซึ่งในขั้นนี้เราจะไม่สามารถตรวจสอบพบผู้บุกรุกได้ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ บริการ whois ทั่วไปบนอินเทอร์เน็ตเพื่อใช้ค้นหาข้อมูลของเครือข่าย คำสั่ง nslookup หรือ dig เพื่อหาชื่อเครื่องคอมพิวเตอร์ในเครือข่าย

2.7.2 การสำรวจระบบ (Scanning)

ผู้บุกรุกจะขยายการสำรวจระบบเป้าหมาย เพื่อหาช่องทางในการเข้าสู่ระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การ ping กวาดไปทั้งระบบเพื่อดูว่ามีเครื่องไหนทำงานอยู่ การสำรวจพอร์ต TCP/UDP บนเครื่องเป้าหมายเพื่อตรวจสอบดูพอร์ตต่างๆที่เครื่องเป้าหมายเปิดให้บริการไว้ และการตรวจสอบระบบปฏิบัติการที่ใช้ ซึ่ง ณ จุดนี้สิ่งที่ผู้บุกรุกกระทำยังเป็นพฤติกรรมปกติที่เกิดขึ้นได้บนระบบเครือข่ายและยังไม่มีสิ่งใดระบุได้ว่าเป็นการบุกรุก แต่ระบบตรวจสอบ ผู้บุกรุกบนเครือข่ายจะสามารถบอกได้ว่ามีใครบางคนกำลังสำรวจระบบของเราอยู่ แต่ยังไม่ได้ทำอะไร

2.7.3 การสำรวจภายในระบบ (Enumeration)

เมื่อผู้บุกรุกเริ่มเจาะระบบเข้ามาทางรูโหว่ที่ตรวจพบเจอของระบบ ก็จะเริ่มทำการสำรวจรายชื่อผู้ใช้งานระบบหรือการแบ่งปันทรัพยากรภายในระบบที่มีการป้องกันไม่ดีนัก เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ List user accounts, List file shares และ Identify applications

2.7.4 การได้รับสิทธิ์ในการใช้งานระบบ (Gaining access)

เมื่อผู้บุกรุกมาถึงจุดนี้และได้ข้อมูลเพียงพอแล้ว ก็จะพยายามทำการให้ได้มาซึ่งสิทธิ์ในการใช้งานระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ การดักดูรหัสผ่าน และการทำให้เกิด Buffer overflows

2.7.5 การยกระดับสิทธิ์การใช้งานระบบ (Escalating privilege)

ถ้าสิทธิ์การใช้งานระบบที่ผู้บุกรุกได้มาจากในขั้นตอนที่แล้วเป็นเพียงระดับผู้ใช้งานทั่วไป ผู้บุกรุกจะพยายามยกระดับสิทธิ์การใช้งานเพื่อให้ได้มาซึ่งความสามารถในการควบคุมได้ทั้งระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ การแคร็ก รหัสผ่าน (Password cracking) และการใช้ประโยชน์จากรูโหว่ต่างๆของระบบ

2.7.6 การลักลอบใช้งานระบบ (Pilfering)

เมื่อผู้บุกรุกได้รับสิทธิ์ในการใช้งานระบบก็มักจะลักลอบใช้งานระบบบางอย่างเพื่อสร้างความเชื่อใจต่อระบบหรือแสวงหาผลประโยชน์จากสิทธิ์ที่ตนได้รับ เช่นแอบสร้างบัญชี

ผู้ใช้ใหม่ที่ถูกต้องไว้สำหรับในการใช้งานเอง ขโมยรหัสผ่านข้อมูลที่สำคัญของผู้ใช้ในระบบ หรือการเปลี่ยนแปลงแก้ไขไฟล์หรือค่าฟอนฟิกูเรชั่นต่างๆของระบบ เป็นต้น

2.7.7 การลบหลักฐาน (Covering Tracking)

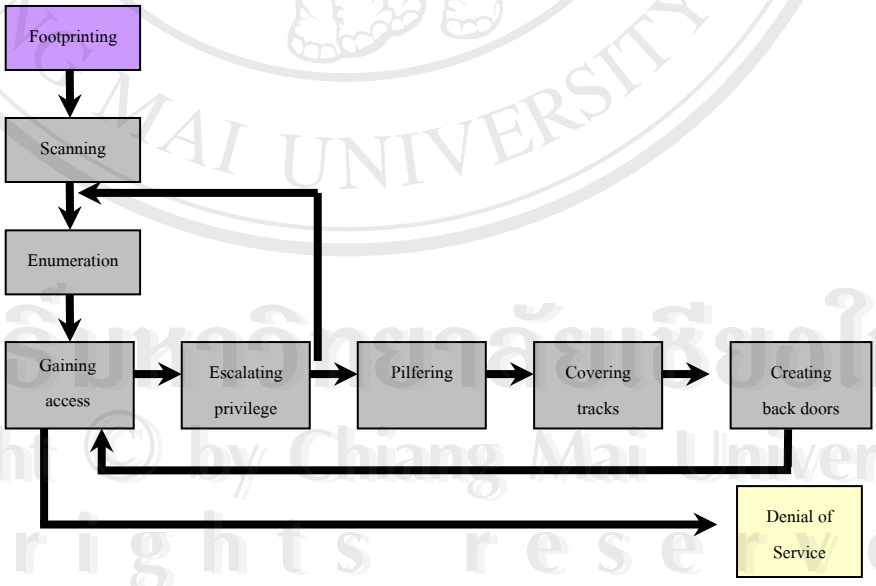
เมื่อผู้บุกรุกแน่ใจว่าระบบเป้าหมายอยู่ในการควบคุมของตนแล้ว ก็จะทำการซ่อนหรือลบหลักฐานที่ใช้ในการเข้าสู่ระบบอย่างผิดปกติของตน เพื่อหลีกเลี่ยงการถูกผู้ดูแลระบบตัวจริงตรวจจับได้ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การเข้าไปลบในล็อคไฟล์ (Log file) ซึ่งเก็บสถานะการใช้งานต่างๆของระบบไว้

2.7.8 การสร้างช่องทางลับ (Creating back door)

ผู้บุกรุกมักจะทำการสร้างช่องทางลับทิ้งไว้ในระบบ เพื่อให้แน่ใจว่าสามารถกลับเข้ามาได้อีกครั้งตามที่ตนต้องการ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การสร้างบัญชีผู้ใช้ใหม่ การลงโปรแกรมประเภทที่สามารถควบคุมจากระยะไกลไว้ หรือลงโปรแกรมประเภทโทรจันไว้

2.7.9 การทำให้ระบบทำงานผิดพลาด (Denial of Service)

ถ้าผู้บุกรุกไม่สามารถบุกรุกเข้ามายังระบบได้สำเร็จ ก็อาจจะใช้ประโยชน์จากรูโหว่ของระบบในการทำให้ระบบทำงานผิดพลาดหรือไม่สามารถให้บริการได้ตามปกติ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ SYN flood, ICMP techniques, Identical src/dst, SYN requests, Overlapping fragment/offset bugs, Out of bound TCP option (OOB) และ Ddos เป็นต้น



รูปที่ 2.7 แสดงขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ

รูปแบบในการบุกรุกเข้าสู่เครือข่ายคอมพิวเตอร์

Robert Graham (2000) แบ่งได้เป็น 3 ประเภทหลักๆได้ดังนี้

การสำรวจระบบ (Reconnaissance) เป็นการสำรวจเป้าหมายขั้นต้นของผู้บุกรุก เพื่อที่จะนำข้อมูลนั้นมาวิเคราะห์หาช่องโหว่ในการบุกรุกเข้ามายังระบบ โดยทั่วไปจะไม่ส่งผลกระทบต่อระบบ เพราะยังไม่ใช่การโจมตี แต่เป็นเพียงกระบวนการเริ่มต้นของการบุกรุกเท่านั้น การสำรวจระบบนั้นทำได้หลายวิธีด้วย วัตถุประสงค์และเทคนิคที่แตกต่างกัน ซึ่งหากเรารู้และตรวจผลของการกระทำได้แต่เนิ่นๆ ย่อมทำให้สามารถเพิ่มความระมัดระวังและเตรียมพร้อมก่อนการถูกบุกรุกจริงได้ อีกนัยหนึ่งคือถ้าเราทราบว่าระบบของเรามีจุดที่ถูกสำรวจได้ง่ายก็จะสามารถป้องกันส่วนนั้นได้ โดยการสำรวจนั้นสามารถแบ่งได้เป็น 3 แบบ คือ

การสำรวจเครือข่าย (Network reconnaissance) เพื่อตรวจสอบเครือข่ายเป้าหมาย ผลที่ได้จะบอกถึงจำนวนและลักษณะ การใช้งานของเครื่องที่มีอยู่ในเครือข่ายนั้น

การสำรวจเครื่อง (Host reconnaissance) เพื่อวิเคราะห์รายละเอียดในแต่ละเครื่องที่คาดว่าจะเจาะเข้าไปได้โดยง่าย ว่ามีพฤติกรรมการใช้งานเป็นอย่างไร ลักษณะจะประกอบด้วยการสำรวจที่สำคัญดังนี้คือ การสำรวจพอร์ต การสำรวจข้อมูลระบุแอพพลิเคชั่น และการสำรวจข้อมูลระบบปฏิบัติการ

การสำรวจแอพพลิเคชั่น (Application reconnaissance) ได้แก่การสำรวจหาแอพพลิเคชั่นเฉพาะเจาะจงที่ทราบช่องโหว่อยู่แล้วหรือการหาโปรแกรมโทรจัน(Trojan)หรือช่องทางลับ(Back doors)ต่างๆ

การใช้ประโยชน์จากระบบ (Exploits) ผู้บุกรุกใช้ประโยชน์จากคุณลักษณะที่ซ่อนอยู่หรือข้อผิดพลาดต่างๆ (Bugs) เพื่อให้ได้มาซึ่งเข้าถึงระบบ ตัวอย่างของลักษณะนี้ได้แก่บัฟเฟอร์โอเวอร์โฟล (Buffer Overflow) การส่งคำสั่งที่มีลักษณะบุกรุก (Unexpected Combination) และอินพุตที่ผิดปกติ (Unhandled Input)

การทำให้ระบบทำงานผิดพลาด (Denial of Services) หมายถึงการกระทำใดๆ ที่ทำให้ระบบเป้าหมายทำงานผิดพลาดหรือไม่สามารถ ให้บริการตามปกติต่อไปได้อีก โดยทั่วไปจะเป็นการโจมตีที่พอร์ตของ TCP/IP ซึ่งเชื่อมต่อกับบริการที่รองรับพอร์ตนั้นๆ ดังนั้นการโจมตีพอร์ตจึงเท่ากับการโจมตีบริการของระบบนั่นเอง ซึ่งการโจมตีแบบนี้ถือเป็นความเสียหายที่รุนแรงมากในระบบที่ต้องให้บริการข้อมูลที่รวดเร็ว

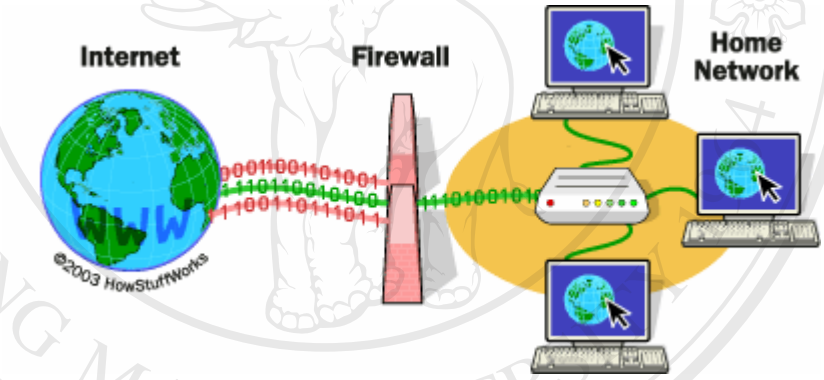
2.8 เทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์

ปัจจุบันได้มีการพัฒนาเทคโนโลยีออกมามายมากเพื่อช่วยในการรักษาความปลอดภัยระบบและข้อมูลสารสนเทศจากบรรดาผู้บุกรุกทั้งหลาย โดยเทคโนโลยีเหล่านี้จะใช้ในการป้องกัน

การบุกรุก ตรวจสอบพฤติกรรมที่ผิดปกติหรือน่าสงสัย และการตอบสนองต่อเหตุการณ์ที่สร้างความไม่ปลอดภัยเหล่านั้น ซึ่งสามารถแบ่งได้เป็นสองประเภทหลักๆคือเทคโนโลยีทางด้านปฏิบัติการ (Operational techonology) และการเข้ารหัสลับ (Cryptography) จุดประสงค์ของการรักษาความปลอดภัยโดยใช้เทคโนโลยีทางด้านปฏิบัติการนั้นคือเพื่อป้องกันและรักษาความพร้อมใช้งานของแหล่งข้อมูล ส่วนเทคโนโลยีทางด้านการเข้ารหัสลับคือเพื่อการรักษาความลับ ความสมบูรณ์ และการพิสูจน์ตัวตนเพื่อเข้าใช้งานแหล่งข้อมูล โดยในเอกสารรายงานการค้นคว้าอิสระฉบับนี้จะขอกล่าวถึงแต่เทคโนโลยีทางด้านปฏิบัติการเฉพาะบางส่วนเท่านั้น

2.8.1 ไฟร์วอลล์ (Firewall)

Ronald L. Krutz (2001) โดยพื้นฐานแล้วไฟล์วอลล์เปรียบเสมือนกำแพงกั้นกลางระหว่างเครือข่ายสองเครือข่ายเพื่อป้องกันการเข้าไปใช้งานเครือข่ายที่ต้องการปกป้องตามนโยบายที่ได้กำหนดไว้



รูปที่ 2.8 แสดงไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน

ชนิดของไฟร์วอลล์

2.8.1.1 Packet Filter เป็นรูปแบบไฟล์วอลล์ที่เก่าแก่ที่สุดแบบหนึ่ง โดยมักจะอาศัยกาทำงานของอุปกรณ์เครือข่ายที่เราเรียกกันว่า Router (เราเตอร์) โดย Router หน้าที่หลักของ Router คือทำการค้นหาเส้นทางและส่งต่อ Packet (ข้อมูลชิ้นเล็กๆที่เดินทางในเครือข่าย) ไปยังเครือข่ายอื่นๆ

รูปที่ 2.9 แสดงRouter ทำหน้าที่ Packet Filtering

Router จะเสมือนเป็นตัวเชื่อมเครือข่ายภายนอกเข้ากับเครือข่ายภายใน และด้วยหลักการทำงานของ Router นี่จึงมีการพัฒนาคุณสมบัติเพิ่มเติมในการให้ Router ตรวจสอบ Packet ก่อนที่จะรับหรือส่งเทียบกับกฎเกณฑ์ที่ได้กำหนดไว้ ถ้าหาก Packet ชิ้นไหนทำตามกฎเกณฑ์ที่ตั้งไว้ก็สามารถยอมรับให้รับเข้ามาในเครือข่าย หรือ ส่งออกไปนอกเครือข่ายได้ ซึ่งกฎที่ตั้งไว้ใน Router นั้นเรามักจะเรียกว่า Access Control Lists (ACLs)

วิธีการจะพิจารณา Packet ว่าถูกต้องตามกฎที่วางไว้รึไม่ Router จะทำการตรวจสอบข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของPacketที่ผ่านเข้ามา เทียบกับกฎที่กำหนดไว้และตัดสินว่าควรจะทิ้ง(drop)Packetนั้นไปหรือว่าจะอนุญาต (accept) ให้Packetนั้นผ่านไปได้

ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของ อินเทอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเทอร์เน็ต โมดล ซึ่งในอินเทอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้

(1) ไอพีต้นทาง

(2) ไอพีปลายทาง

(3) ชนิดของโปรโตคอล (TCP UDP และ ICMP)

และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

(1) พอร์ตต้นทาง

(2) พอร์ตปลายทาง

(3) แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของPacket TCP)

(4) ชนิดของ ICMP message (ในPacket ICMP)

ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่Packetนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมPacketที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของPacket หรือ ชนิดของ ICMP ในPacket ICMP) ได้ เช่น ห้าม

Packetทุกชนิดจาก crack.cracker.net เข้ามายังเครือข่าย 203.154.207.0/24 ห้ามPacketที่มีไอพีต้นทางอยู่ในเครือข่าย 203.154.207.0/24 ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

(1) เราเตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว)

(2) คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์

ซึ่งจะมีข้อได้เปรียบเสียเปรียบกันดังนี้

ตารางที่ 2.1 แสดงการเปรียบเสียเปรียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ Packet Filtering

	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลางจำนวนอินเตอร์เฟสน้อยอาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดีของ Packet Filtering

(1) ไม่ขึ้นกับแอพพลิเคชัน

(2) มีความเร็วสูง

(3) รองรับการขยายตัวได้ดี

ข้อเสียของ Packet Filtering

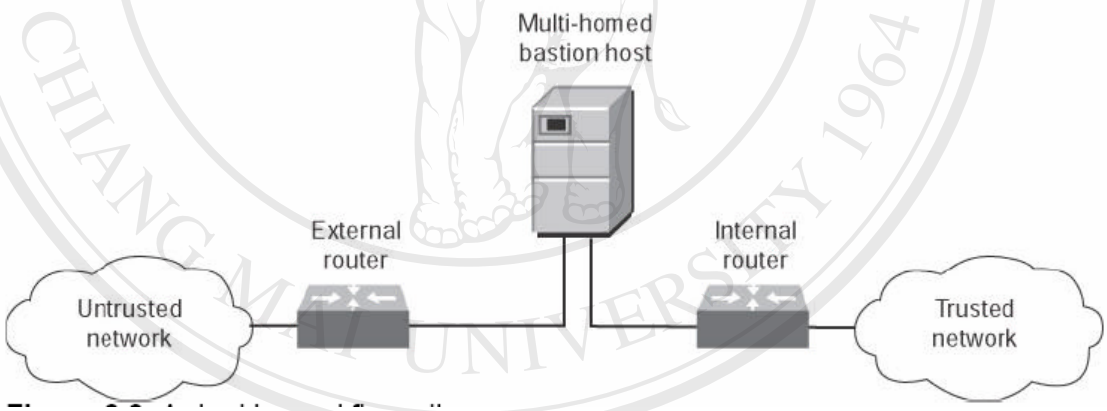
บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ ซึ่งมีการทำงานแบบไดนามิกพอร์ต อย่างไรก็ตามไฟล์วอลล์ประเภทนี้ค่อนข้างใช้งานลำบากเนื่องจาก การเปลี่ยนแปลงกฎหรือตั้งกฎมีความซับซ้อนและยุ่งยาก นอกจากนี้ยังมีจุดอ่อนด้านอื่นๆ อีกเช่น ไม่มีการตรวจสอบสิทธิที่มากพอในการใช้งาน กฎเกณฑ์ที่ตั้งไว้อย่างซับซ้อนจะมีผลต่อประสิทธิภาพ

การทำงานของตัว Router เอง และบางครั้งมักมีการนำไฟล์วอลล์แบบนี้มากั้นเขตพิเศษที่เรามักจะเรียกกันว่า DMZ (Demilitarized zone)

2.8.1.2 Proxy หรือ Application Gateway

เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่าง เครือข่าย 2 เครือข่าย ทำหน้าที่เพิ่มความปลอดภัยของระบบเครือข่ายโดยการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการ ตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)

เมื่อไคลเอนต์ต้องการใช้บริการภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อPacketให้หรือไม่



รูปที่ 2.10 แสดงใช้ Dual-homed Host เป็น Proxy Server

ข้อดีของ Proxy

1. มีความปลอดภัยสูง
2. รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสียของ Proxy

1. ประสิทธิภาพต่ำ
2. แต่ละบริการมักจะต้องการโปรเซสของตนเอง
3. สามารถขยายตัวได้ยาก

2.8.1.3 Stateful Inspection Technology

โดยปกติแล้ว Packet Filtering แบบธรรมดา (ที่เป็น Stateless แบบที่มีอยู่ในเราเตอร์ทั่วไป) จะควบคุมการเข้าออกของPacketโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละPacket นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า Packetนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นPacketที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นPacketที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้Packetผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของPacket (message content) และข้อมูลที่ได้จากPacketก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าPacketใดเป็นPacketที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology

1. Check Point Firewall-1
2. Cisco Secure Pix Firewall
3. SunScreen Secure Net
4. และส่วนที่เป็น open source แจกฟรี ได้แก่
5. NetFilter ใน Linux (Iptables ในระบบปฏิบัติการลีนุกซ์เคอร์เนล 2.4 เป็นต้นไป)

2.8.2 ระบบตรวจสอบผู้บุกรุก (Intrusion Detection System หรือ IDS)

ร.อ.วิวัต เรืองมี (2548) ระบบตรวจสอบการบุกรุกคือระบบที่ใช้ในการตรวจสอบการใช้งานและความพยายามในการใช้งานคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับและเจตุจำนงค์การใช้งาน ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ 3 ประการคือ การรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน(Availability)

2.8.2.1 ทำไมถึงจำเป็นต้องใช้ระบบตรวจสอบผู้บุกรุก

เมื่อคำนึงถึงเรื่องความปลอดภัยของคอมพิวเตอร์มักเป็นการยากในการมองภาพที่ชัดเจนว่า อะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย เนื่องจากความปลอดภัยของคอมพิวเตอร์เป็นสิ่งที่จับต้องไม่ได้และยากต่อการวัด แต่อย่างไรก็ตามเราสามารถ

เปรียบเทียบความปลอดภัยของคอมพิวเตอร์กับการรักษาความปลอดภัยสถานที่ ในการรักษาความปลอดภัยสถานที่นั้นนอกจากการ จัดบริเวณที่ต้องการรักษาความปลอดภัยให้มีรั้วรอบขอบชิด มีกุญแจที่ใช้ล็อกประตูหรือทางเข้าออก สิ่งหนึ่งที่จะขาดไม่ได้คือการจัดให้มีบุคคลหรืออุปกรณ์ที่คอยตรวจสอบ การละเมิดต่ออุปกรณ์หรือเครื่องกีดขวางที่จัดตั้งเพื่อความปลอดภัย ทั้งนี้เนื่องจากอาจมีผู้ไม่หวังดีพยายามบุกรุกโดยทำลายอุปกรณ์หรือเครื่องกีดขวางดังกล่าวดังนั้นเราจึงต้องอาศัยระบบที่ใช้ตรวจสอบเมื่อมีการทำลายหรือล่วงล้ำต่ออุปกรณ์หรือเครื่องกีดขวางที่ได้ติดตั้งไว้อีกชั้นหนึ่ง ตัวอย่างอุปกรณ์ที่ใช้ตรวจสอบเช่น ระบบสัญญาณเตือนขโมยที่ใช้ควบคู่กับรั้วที่แข็งแรง

ระบบเครือข่ายคอมพิวเตอร์ก็เช่นเดียวกัน บุคคลทั่วไปมักคิดว่าการติดตั้งไฟร์วอลล์ตามลำพังก็สามารถทำให้เครือข่ายคอมพิวเตอร์มีความปลอดภัย แต่อย่างไรก็ตามการติดตั้งไฟร์วอลล์ ให้กับระบบเครือข่ายคอมพิวเตอร์ก็เปรียบเสมือนการสร้างรั้วหรือกำแพงเพื่อตรวจสอบบุคคลที่จะเข้ามาในสถานที่ที่จะการรักษาความปลอดภัยแต่หากมีบุคคลไม่หวังดีสามารถปีนรั้วเข้ามาได้ การรักษาความปลอดภัยโดยใช้รั้วก็หมดความหมาย ดังนั้นในการเพิ่มความปลอดภัยอีกประการหนึ่งคือการใช้ระบบตรวจสอบการบุกรุกซึ่งมีคุณลักษณะที่กล่าวมาในตอนต้น

2.8.2.2 ชนิดของระบบตรวจสอบผู้บุกรุก

Earl Carter (2005) ได้แบ่งประเภทของระบบตรวจสอบผู้บุกรุกสามารถแบ่งได้เป็น 2 ประเภทหลักดังนี้

1) แบ่งตามวิธีการตรวจจับการบุกรุก

ก. Anomaly Detection หรือ Profile-based Detection

การตรวจจับโดยวิธีนี้ต้องอาศัยการสร้างแฟ้มข้อมูล (Profile) ของผู้ใช้หรือกลุ่มของผู้ใช้งานในระบบขึ้นมา เพื่อใช้เก็บพฤติกรรมการใช้งานที่เป็นปกติจากกิจกรรมหรืองานที่ต้องทำอยู่เป็นประจำ แฟ้มข้อมูลเหล่านี้จึงเปรียบเสมือนบรรทัดฐานที่ใช้ในการตรวจจับพฤติกรรมที่ผิดปกติไปจากการทำงานตามปกติของผู้ใช้ในระบบ

ด้วยวิธีนี้ระบบตรวจสอบผู้บุกรุกจะสามารถตรวจจับการบุกรุกได้โดยดูจากพฤติกรรมการที่ผิดไปจากการใช้งานปกติของระบบ ซึ่งจะไม่มีรูปแบบที่แน่นอนสำหรับทุกระบบขึ้นอยู่กับพฤติกรรมการใช้งานปกติของระบบนั้นๆเอง ฉะนั้นการกำหนดบรรทัดฐานของพฤติกรรมปกติในระบบจึงเป็นเรื่องที่สำคัญและละเอียดอ่อนมาก ถ้าระบบสามารถกำหนด

บรรทัดฐานที่ครอบคลุมพฤติกรรมการใช้งานปกติของระบบได้หมด การเกิด False Positive[11] จากระบบตรวจสอบผู้บุกรุกประเภทนี้ก็จะมีโอกาสเกิดขึ้นน้อย ในขณะที่การเกิด False Negative[12] ก็มีโอกาสเกิดขึ้นได้จากการบุกรุกที่มีพฤติกรรมเหมือนการใช้งานตามปกติในระบบ ซึ่งในกรณีนี้แทบจะเป็นไปไม่ได้เลยที่ระบบตรวจสอบผู้บุกรุกประเภทนี้จะสามารถแยกแยะได้ว่าพฤติกรรมใดเป็นการใช้งานตามปกติหรือว่าเป็นบุกรุก

ข. Misuse Detction หรือ Signature-based Detection

เป็นการตรวจจับพฤติกรรมการบุกรุกโดยเปรียบเทียบจากข้อมูลลักษณะเฉพาะ (Signature) ที่ใช้อ้างอิง ซึ่งลักษณะเฉพาะเหล่านี้จะเป็นกลุ่มของกฎต่างๆที่เป็นรูปแบบหรือพฤติกรรมของผู้บุกรุกที่ใช้ในการบุกรุกเข้าสู่ระบบ

ฉะนั้นการกำหนดรูปแบบลักษณะเฉพาะที่ใช้อ้างอิงเปรียบเทียบที่ดีจะสามารถลดโอกาสในการเกิด False Positive ได้ ในขณะที่การป้องกันการเกิด False Negative จะขึ้นอยู่กับการหมั่นปรับปรุงฐานข้อมูลลักษณะเฉพาะเหล่านี้ให้ทันสมัยต่อรูปแบบการบุกรุกที่เกิดขึ้นใหม่ๆอยู่ตลอดเวลา

2) แบ่งตามตำแหน่งในการตรวจจับการบุกรุก

ก. Host-based IDS (HIDS) ทำงานอยู่บนเครื่องคอมพิวเตอร์ที่ต้องการตรวจสอบการบุกรุกเอง โดยตรวจจับการบุกรุกที่เกิดขึ้นในระดับระบบปฏิบัติการ (Operating System) ซึ่งข้อมูลที่ได้จากระบบตรวจสอบประเภทนี้เป็นข้อมูลที่ได้หลังการบุกรุกไปยังเครื่องเป้าหมายแล้วจริงๆเท่านั้น ในขณะที่ระบบตรวจสอบผู้บุกรุกประเภท Network-based IDS จะไม่สามารถทำได้ เพราะการส่งสัญญาณเตือนภัยเมื่อตรวจพบพฤติกรรมที่เข้าข่ายการบุกรุกที่เข้ามายังระบบเครือข่ายทั้งหมด จึงมีแต่ Host-based IDS เท่านั้นที่สามารถตัดสินได้ว่าการบุกรุกที่ตรวจพบครั้งนั้นสำเร็จหรือล้มเหลว

---

[11] False Positive หมายถึงการที่ IDS ตรวจพบการบุกรุกที่เกิดจากกิจกรรมการทำงานปกติ ซึ่งไม่ใช่การบุกรุกจริง ซึ่งการเกิด False Positive จะทำให้เกิดการสูญเสียทั้งเวลาและทรัพยากรของระบบโดยเปล่าประโยชน์

[12] False Negative หมายถึงการที่ IDS ตรวจไม่พบการบุกรุกที่เกิดขึ้นจริง ซึ่งการเกิด False Negative จะให้ผลลัพธ์ที่เลวร้ายกว่า False Positive มาก แต่ก็เป็นการยากที่จะออกแบบ IDS ไม่ให้เกิด False Negative ขึ้น ในขณะที่เราออกแบบให้ระบบมี False Negative ให้น้อยเท่าไหร่ แนวโน้มที่ระบบจะเกิด False Positive ก็มีมากขึ้นเท่านั้น

ข. Network-based IDS (NIDS)ทำงานอยู่บนเครือข่ายจะทำการเฝ้าดูและตรวจสอบข้อมูลPacketต่างๆจะถูกตรวจสอบโดยตัวตรวจจับหรือเซ็นเซอร์ (Sensor) ของระบบ ซึ่งตัวตรวจจับจะมองเห็นเฉพาะPacketที่วิ่งผ่านบนเครือข่ายที่ตัวตรวจจับนั้นติดตั้งอยู่เท่านั้น ซึ่งระบบตรวจสอบประเภทนี้สามารถตรวจสอบการบุกรุกได้ทั้งระบบเครือข่าย ไม่เกิดความยุ่งยากในการติดตั้งระบบตรวจสอบผู้บุกรุกบนเครื่องที่ต้องการตรวจสอบทุกเครื่องเหมือน Host-based IDS และการเก็บบันทึกข้อมูลการบุกรุกที่แยกต่างหาก ทำให้ปลอดภัยจากการทำลายร่องรอยการบุกรุกหลังจากผู้บุกรุกสามารถเข้าสู่ระบบแล้ว

Packet ต่างๆจะเป็นที่สนใจของตัวตรวจจับก็ต่อเมื่อPacketนั้นเข้ากับรูปแบบที่กำหนดไว้ ซึ่งปกติแล้วรูปแบบจะมีอยู่ 3 ประเภท ได้แก่

1. รูปแบบทางตัวอักษร (String signature) ซึ่งอาจบ่งบอกถึงการโจมตี ตัวอย่างเช่น " cat " + + " 7% rhost " อาจทำให้ระบบยูนิกซ์ เกิดช่องโหว่ต่อการโจมตีบนเครือข่ายได้

2. รูปแบบทางพอร์ต (Port signature) เป็นการพยายามติดต่อเข้ามาทางพอร์ตที่รู้จักกันดีและมักจะถูกโจมตี เช่น telnet จะใช้ TCP พอร์ต 23, FTP จะใช้ TCP พอร์ต 21/20, SUNRPC ใช้ TCP/UDP พอร์ต 111 และ IMAP จะใช้ TCP พอร์ต 143 ซึ่งถ้าระบบของเราไม่ได้เปิดพอร์ตดังกล่าว แต่มีการพยายามเชื่อมต่อเข้ามา แสดงว่าPacketดังกล่าว อาจจะมีความประสงค์ร้ายก็ได้

3. รูปแบบทางเงื่อนไขในส่วนเฮดเดอร์ (Header condition signature)เป็นพยายามส่งข้อมูลที่มีลักษณะเป็นอันตรายและผิดกฎของการกำหนดคาในส่วนของเฮดเดอร์ ตัวอย่างที่เห็นได้ชัดคือPacket TCP ซึ่งมีทั้ง SYN และ FIN Flags

2.8.2.3 กลไกระบบตรวจสอบผู้บุกรุก

ระบบตรวจสอบผู้บุกรุกจะทำการวิเคราะห์กิจกรรมต่างที่เกิดขึ้นบนระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ว่าเป็นการบุกรุกหรือความพยายามในการบุกรุกหรือไม่โดยอาศัยค่าต่างๆ อาทิเช่น Network traffic การใช้งาน CPU, I/O,ไฟล์ หรือที่อยู่ของผู้ใช้ โดยใช้แบ่งวิธีวิเคราะห์หลักๆออกเป็น 2 วิธีคือการตรวจสอบกับข้อกำหนดการใช้งานและการตรวจสอบจากสถิติการใช้งาน

ระบบตรวจจับการบุกรุกโดยทั่วไปจะใช้วิธีตรวจสอบกับข้อกำหนดการใช้งาน ทั้งนี้เนื่องจากมีความง่าย มาก กว่าการตรวจสอบจากสถิติซึ่งมักมีกรณีใหม่เกิดขึ้นตลอดเวลา ทำให้การระบุว่าการกระทำนั้นเป็นการบุกรุกมีความยากและอาจเกิดการระบุที่ผิดพลาด (Fault Alarm)

2.9 หลักการพื้นฐานของโปรโตคอล TCP/IP

ในการสื่อสารระหว่างมนุษย์นั้น ต้องใช้ภาษาในการสื่อสาร และภาษาที่ใช้ในการสื่อสารนั้นก็มีความแตกต่างกันไปตามเชื้อชาติ การสื่อสารในชนชาติเดียวกันก็ต้องใช้ภาษาเดียวกัน แต่ในการสื่อสารกับชนชาติอื่น ต้องใช้ภาษาที่สามารถเป็นสื่อกลางได้เช่น ภาษาอังกฤษเป็นต้น

คอมพิวเตอร์ก็เช่นกัน ในการที่จะให้คอมพิวเตอร์ทำการติดต่อสื่อสารซึ่งกันและกันได้นั้น ก็ต้องใช้ภาษาในการติดต่อสื่อสารเช่นกัน แต่ในทางคอมพิวเตอร์นั้นจะไม่เรียกว่าภาษาแต่จะถูกเรียกว่า โปรโตคอล (Protocol) และเช่นเดียวกันโปรโตคอลที่ใช้ในการสื่อสารของคอมพิวเตอร์ก็มีอยู่หลายโปรโตคอลด้วยกัน การที่จะให้คอมพิวเตอร์สามารถสื่อสารกันได้ก็ต้องใช้โปรโตคอลเดียวกันด้วย และชุดโปรโตคอลที่เป็นมาตรฐานที่ใช้งานทางด้านอินเทอร์เน็ตก็จะเป็นชุดโปรโตคอลที่เรียกว่า TCP/IP

ดังนั้น TCP/IP ก็คือชุดโปรโตคอลที่ถูกพัฒนาขึ้นมาเป็นมาตราฐานในการติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ ทำให้เครื่องคอมพิวเตอร์สามารถใช้งานทรัพยากรเช่น แฟ้มข้อมูล หรือ เนื้อที่ไดรว์ร่วมกันได้ โดยผ่านระบบเครือข่าย

ในความเป็นจริงแล้ว TCP/IP ประกอบไปด้วยโปรโตคอลที่แตกต่างกันในหลายชั้นเลเยอร์ด้วยกัน เช่น TCP (Transmission Control Protocol), IP (Internet Protocol) เป็นต้น ซึ่งเป็นโปรโตคอลที่เป็นที่รู้จักและใช้งานกันอย่างแพร่หลาย ดังนั้นในปัจจุบันเมื่อกล่าวถึงการใช้งานอินเทอร์เน็ตจึงมักจะเรียกชุดโปรโตคอลนี้รวมกันว่า TCP/IP

2.9.1 ลำดับชั้นการทำงานของโปรโตคอล

ในการศึกษาหลักการทำงานของโปรโตคอลในระบบเครือข่าย(Network Protocols) ใดๆ จะเริ่มต้นด้วยการมองการทำงานของมันเป็นชั้น ๆ หรือที่เรียกว่าเลเยอร์ (Layer) การทำงานทั้งหมดของโปรโตคอลจะประกอบไปด้วยหลาย ๆ เลเยอร์ซึ่งนำมาวางซ้อนกันได้ออกมาเป็นรูปแบบที่เราเรียกว่า Protocol Stack แต่ละเลเยอร์ก็จะมีหน้าที่การทำงานที่ชัดเจนและไม่เกี่ยวข้องกัน แต่ละชั้นจะรู้เพียงวิธีการส่งข้อมูลไปยังชั้นอื่นๆ จะไม่รู้ถึงการทำงานข้างในเลย แต่ละชั้นจะมีการแบ่งการทำงานออกเป็นโปรโตคอลต่างๆจำนวนไม่เท่ากัน ทำให้เป็นการยากที่จะระบุว่าโปรโตคอลในระบบเครือข่ายโดยรวมแล้วมีทำงานกี่เลเยอร์ แต่ก็มีมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไป เรียกว่า Open System Interconnect (OSI) Reference Model ซึ่งทำการแบ่งการทำงานของโปรโตคอลในระบบเครือข่ายออกเป็น 7 เลเยอร์ ดังนี้

7	**Application Layer**
6	**Presentation Layer**
5	**Session Layer**
4	**Transport Layer**
3	**Network Layer**
2	**Data Link Layer**.
1	**Physical Layer**.

รูปที่ 2.11 โมเดล OSI[13]

แต่ละชั้นก็มีข้อกำหนดและการทำงานที่แน่นอนและไม่เกี่ยวข้องกับชั้นอื่น สำหรับการศึกษาโปรโตคอล TCP/IP นั้นบางที่ก็จะไม่อ้างอิง OSI Reference Model เนื่องจากมีการแบ่งชั้นการทำงานอย่างละเอียดทำให้เข้าใจยาก ดังนั้นจึงมีจะสร้างโมเดลขึ้นมาใหม่เพื่อให้ในการอธิบายการทำงานของโปรโตคอล TCP/IP โดยแบ่งออกเป็น 4 ชั้นดังนี้

Application Layer	Telnet, FTP, e-mail, etc
Transport Layer	TCP, UDP
Internet Layer	IP, ICMP, IGMP
Link Layer	Device driver and interface card

รูปที่ 2.12 โมเดล Internet Reference TCP/IP[14]

[13] Obert N. Myhre, CCNA Certification: Routing Basics for Cisco Crtified Ntwork Associates Exam 640-407 (NJ : Prentice Hall PTR, 1999), pp. 6

[14] W. Richard Stevens, TCP/IP Illustrated, Volume 1 The Protocols (Bangalore : Addison Wesley Longman, Inc, 1999), pp. 6

1.) เลเยอร์ Application ทำหน้าที่จัดการเกี่ยวกับแอพริเคชันหรือโปรแกรมต่างๆที่ถูกใช้งานโดยผู้ใช้ ตัวอย่างของแอพริเคชันที่ใช้งานโดยทั่วไป เช่น

ก. Telnet หรือ Remote login เป็นบริการให้ผู้ใช้งานสามารถเรียกใช้งานเครื่องคอมพิวเตอร์จากเครื่องคอมพิวเตอร์ที่อยู่ห่างออกไปได้

ข. FTP (File Transfer Protocol) เป็นบริการในการโอนถ่ายแฟ้มข้อมูลระหว่างเครื่องคอมพิวเตอร์

ค. SMTP (Simple Mail Transfer Protocol) เป็นบริการในการรับ-ส่งจดหมายอิเล็กทรอนิกส์

ง. DNS (Domain Name Service) เป็นบริการแปลงชื่อจากรูปแบบของโดเมนเนม เช่น cmu.chiangmai.ac.th เป็นแบบไอพีแอดเดรส เช่น 202.28.249.1 หรือทำกลับกันในการแปลงไอพีแอดเดรสไปเป็นชื่อโดเมนเนม

จ. NFS (Network File System) เป็นบริการในการใช้ทรัพยากร เช่น แฟ้มข้อมูลหรือเนื้อที่ระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย

2.) เลเยอร์ Transport ทำหน้าที่ในการจัดเตรียมช่องทางในการส่งผ่านข้อมูลของเลเยอร์ Application ระหว่างโฮสต์ ในเลเยอร์ Transport นี้ยังแบ่งออกเป็น 2 โปรโตคอล ได้แก่

ก. UDP (User Datagram Protocol)

มีหน้าที่เพียงแค่ทำการจัดส่งข้อมูลที่เรียกว่า Datagram ไปยังโฮสต์ปลายทางโดยไม่มีการตรวจสอบกับปลายทางว่ามีผู้รับหรือไม่ ดังนั้น Datagram ที่ถูกส่งไปอาจจะไม่ถึงปลายทางก็ได้ โดยปกติแล้วถ้าหากใช้โปรโตคอลนี้แล้วต้องการตรวจสอบว่าข้อมูลถึงปลายทางจริงหรือไม่ จะให้โปรแกรมในเลเยอร์ Application ทำหน้าที่ในการตรวจสอบแทน

ข. TCP (Transmission Connection Protocol)

มีหน้าที่ในการจัดเตรียมเกี่ยวกับความถูกต้องแน่นอนของข้อมูลระหว่างโฮสต์ มีการตรวจสอบข้อมูลระหว่างต้นทางและปลายทาง รวมถึงการจัดการแบ่งข้อมูลจากแอพริเคชันให้มีขนาดพอเหมาะกับเลเยอร์ Network กำหนด Time out ของสัญญาณตอบรับจากโฮสต์ปลายทางและอื่นๆ

3.) เลเยอร์ Network หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Internet ทำหน้าที่จัดการเกี่ยวกับการส่งผ่านข้อมูลไปมาของPacketในเครือข่ายหรือทำการจัดการเกี่ยวกับการหาเส้นทาง (Routing) นั้นเอง โปรโตคอลในเลเยอร์นี้ได้แก่

ก. IP (Internet Protocol)

เป็นโปรโตคอลหลักที่ทำงานอยู่ในโปรโตคอล TCP/IP ทำหน้าที่ในการติดต่อกับโปรโตคอลต่างๆทั้ง TCP, UDP, ICMP, และ IGMP ในรูปของไอพีดาตาแกรม (IP Datagram) ซึ่งการส่งข้อมูลนั้นจะเป็นการส่งแบบ Connectionless คือจะไม่มีการตรวจสอบปลายทางว่ามีผู้รับหรือไม่ โปรโตคอล IP จะทำหน้าที่เพียงส่งข้อมูลแต่ละดาตาแกรมออกไป และถ้าหากเกิดความผิดพลาดบางอย่างเช่น เกิดปัญหาที่เราเตอร์ก็จะทำเพียงแค่การส่งข้อความด้วย ICMP กลับไปบอกแก่ต้นทางเท่านั้น การตรวจสอบข้อมูลจะเป็นหน้าที่ของเลเยอร์ที่อยู่สูงกว่าขึ้นไป

ข. ICMP (Internet Control Message Protocol)

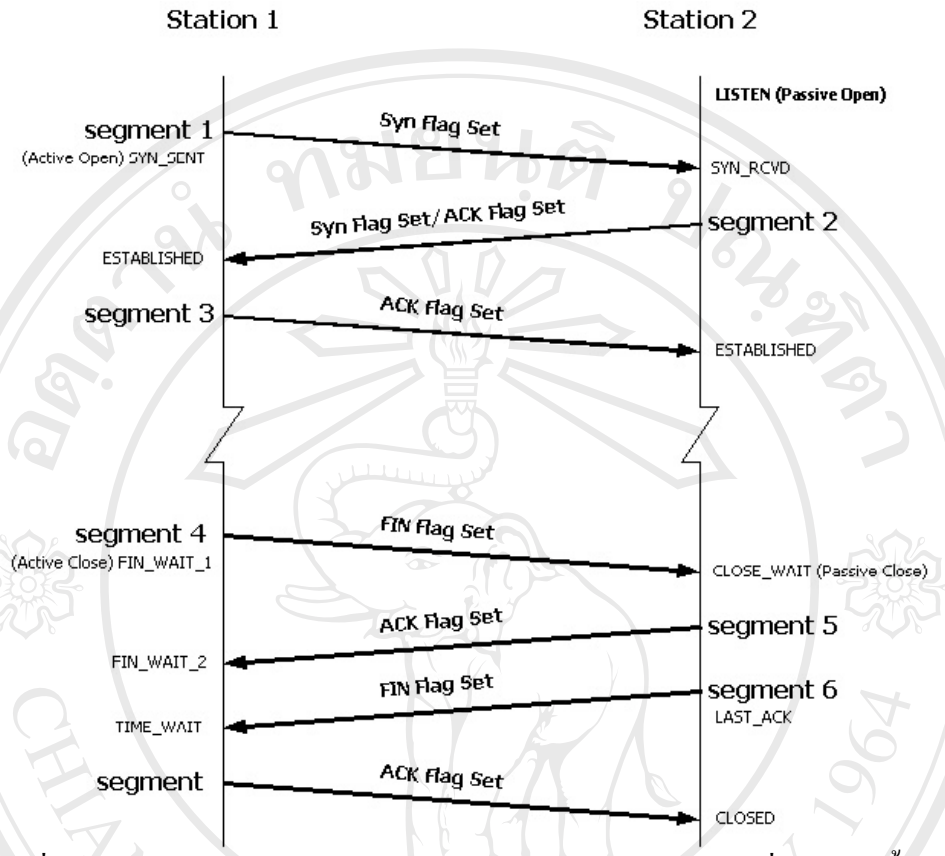
เป็นส่วนประกอบของ IP ซึ่งถูกใช้โดยเลเยอร์ IP ในการเปลี่ยนข้อมูลความผิดพลาดที่สำคัญต่างๆ อันเกิดจากเลเยอร์ IP ของโฮสต์หรือเราเตอร์ต่างๆ ให้เป็นข้อความโดยปกติแล้ว ICMP จะถูกใช้โดยเลเยอร์ IP แต่ก็สามารถถูกใช้โดยเลเยอร์ Application ก็ได้ ตัวอย่างเช่น โปรแกรม Ping และ Traceroute ซึ่งคำสั่งทั้งคู่เป็นแอพริเคชันที่ใช้โปรโตคอล ICMP

ค. IGMP (Internet Group Management Protocol)

เป็นโปรโตคอลที่ถูกใช้งานโดยโฮสต์และเราเตอร์ที่สนับสนุนการทำงานแบบ มัลติแทสกิง (Multicasting) ทำหน้าที่ในการเก็บและส่งข้อมูลเกี่ยวกับมัลติแทสกิงกรุ๊ปของโฮสต์ต่างๆในระบบเครือข่าย โปรโตคอล IGMP เป็นโปรโตคอลที่คล้ายกับ ICMP คือเป็นโปรโตคอลที่เป็นส่วนประกอบของเลเยอร์ IP และข้อมูลถูกส่งออกสู่เครือข่ายด้วยไอพีดาตาแกรม จุดที่แตกต่างจากโปรโตคอลอื่นๆคือ IGMP message จะมีขนาดคงที่เสมอ

4.) เลเยอร์ Link หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Data-link โดยปกติแล้วจะหมายถึงไดฟ์เวอร์ของอุปกรณ์ ระบบปฏิบัติการ เน็ตเวิร์คอินเตอร์เฟสการ์ด (Network Interface Card) ของคอมพิวเตอร์ รวมถึงรายละเอียดเกี่ยวกับเคเบิ้ลอินเตอร์เฟส (Cable Interface) ด้วย

2.9.2 สถานะของโปรโตคอล TCP ในการเชื่อมต่อการทำงาน



รูปที่ 2.13 แสดงลำดับและสถานะต่างๆของโปรโตคอล TCP ในการเริ่มต้นและสิ้นสุดการเชื่อมต่อ

15

ตารางที่ 2.2 แสดงสถานะในการรับส่งของโปรโตคอล TCP

3-Character abbreviation	คำอธิบาย
URG	The urgent pointer is valid
ACK	The acknowledgement number is valid
PSH	Push data to receiving process as soon as possible
RST	Reset connection
SYN	Synchronize sequence numbers
FIN	Sender is finished sending data

[15] W. Richard Stevens, TCP/IP Illustrated, Volume 1 The Protocols (Bangalore : Addison Wesley Longman, Inc, 1999), pp. 242